AP Computer Science Principles Study Guide

Chapter 1: Digital Information

1.1 The Binary System

- **Binary** is a base-2 numeral system that represents numeric values using two symbols: 0 and 1. It's the foundation of how computers store and process data.

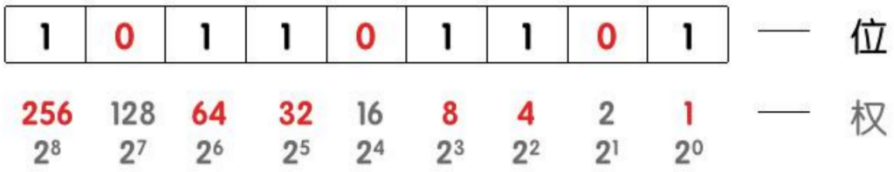
- **Bits**: The smallest unit of data in a computer, represented as either 0 or 1.

- **Bytes**: A group of 8 bits. One byte can represent 256 different values (2^8).

0	1	1	1
+/-	4	2	1
sign	2^2	2^1	2^0

(This represents +(4+2+1)=7)

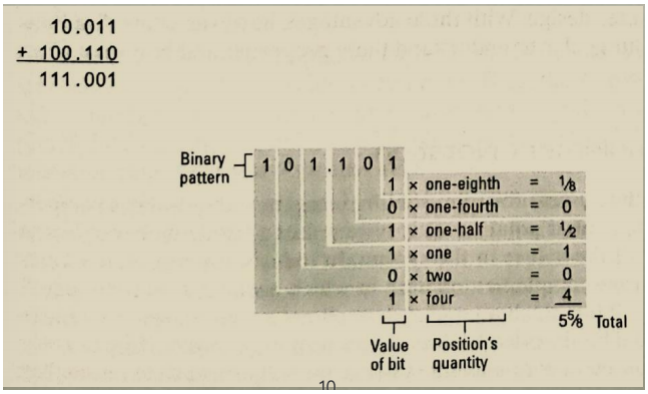
-**Binary to Decimal**:



十转二：有权添一，无权补零

365 - 256 = 109 - 64 = 45 - 32 = 13 - 8 = 5 - 4 = 1

- **Binary Addition**: Similar to decimal addition but only uses 0 and 1.



- **Limitations of storing numbers**: The example above has a maximum storage of 7, therefore:

```
var x = 7;
var y = x + 1;
```

This will result in an overflow on a 4-bit computer.

- **Round-off errors**: As computers cannot store infinitely repeating sequences, chopping it off or rounding it to the nearest floating number is the ideal solution:

```
>>> result = 0.1 + 0.1 + 0.1
>>> print(result)
0.30000000000000004
```

1.2 Representing Text

- **ASCII**: A character encoding standard for electronic communication, where each letter, number, or symbol is represented by a 7-bit binary number.

  - Example: The letter "A" is represented by `1000001` in ASCII.

- Unicode: A more comprehensive character encoding that includes characters from all languages, allowing for representation of global text.

- **UTF-8** describes every character from the Unicode standard using 1-6 bytes, the number of 1 bits at the beginning of the byte determine how many bytes following it represent the same character.

Number of bytes	Byte 1	Byte 2	Byte 3	Byte 4
1	0xxxxxxx			
2	110xxxxx	10xxxxxx		
3	1110xxxx	10xxxxxx	10xxxxxx	
4	11110xxx	10xxxxxx	10xxxxxx	10xxxxxx

1.3 Analogue & Digital

-

Analog Data	Digital Data
attempt to be continous	take discrete values in a certain interval
clocks with hands 	digital clocks 

7

Why do we use Binary in digital devices: Easy & reliable if the data only had to represent one of two status.

1.4Representing Images and Sounds

- Pixel and Resolution:

  - Pixel: The smallest unit of a digital image, often represented by a grid of tiny squares.

  - Resolution: The number of pixels in a given image. Higher resolution means more pixels and a clearer image.

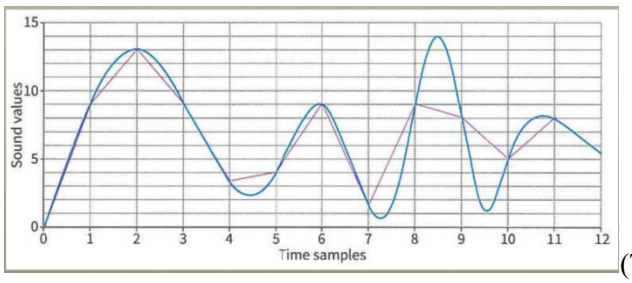
- Color Representation:

  - RGB Model: Each pixel's color is represented by a combination of red, green, and blue values, often stored as three numbers (one for each color channel).

  - Example: Pure red is `(255, 0, 0)` in RGB.

- Sound waves

Sample rates are measured in hertz.1 hertz equals 1 sample per second(pretty low).



(This looks significantly different from the original sample)

1.5 Data Compression

- What is Data Compression?: The process of reducing the size of a file or dataset to save space or speed up transmission.

  - Lossless Compression: Data is compressed without any loss of information (e.g., ZIP files).

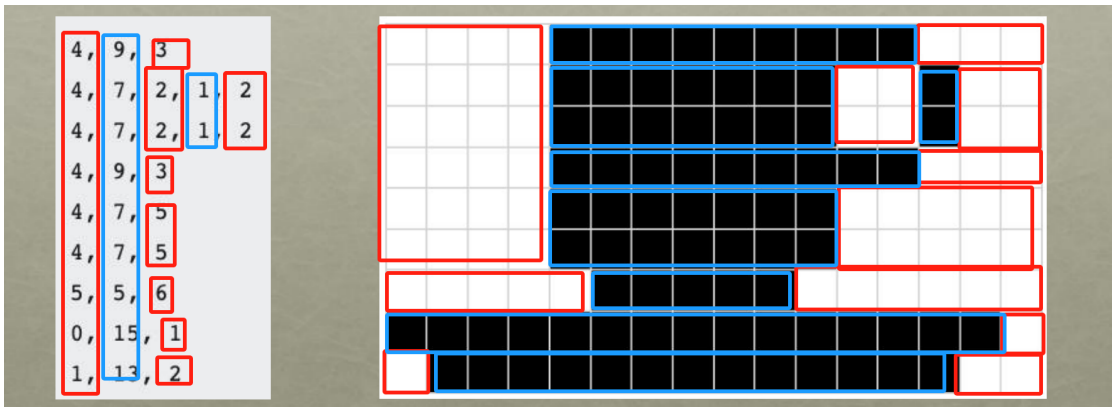
  - Lossy Compression: Data is compressed by losing some information, commonly used for images and sound (e.g., JPEG, MP3).(Specifically for audio, the inaudible sounds are discarded)

- Compression Algorithms: 1. replace repeated sequences 2. store replacements for reconstruction

e.g. “To be or not to be, that is the question” --> “@ # or not @ #, $at is $e question”

To=@, be = #, th=$

-RLE:



- Trade-offs of Compression:

  - Lossy compression reduces file size significantly but sacrifices quality.

  - Lossless compression maintains quality but doesn’t always compress data as much.

Chapter 2: The Internet

1. Introduction to Computer Networks

What is a Computer Network?

A system that connects multiple computers and devices to share information and resources.

Types of networks:

Local Area Network (LAN): Covers a small geographic area, like a home or office.

Wide Area Network (WAN): Covers larger areas, such as cities or even countries.

The Internet: A global network of interconnected computers that enables communication and resource sharing worldwide.

---

2. Network Topologies

Ring Topology:

Each device is connected to two other devices, forming a circular path. Data travels in one direction. If one connection fails, the entire network can be disrupted.

Mesh Topology:

Every device is connected to every other device. Highly reliable but expensive to set up.

Star Topology:

All devices are connected to a central hub. If the hub fails, the entire network goes down, but individual device failure does not affect the network.

Bus Topology:

All devices share a single communication line or bus. Simple and cost-effective, but the entire network goes down if the bus fails.

Tree Topology:

A combination of bus and star topologies, organized in a hierarchical structure.

---

3. IP Addresses and Routers

IP Addressing

What is an IP Address?

Types of IP Addresses:

IPv4:

Format: Consists of four octets (8 bits each) written in decimal form and separated by periods (e.g., 192.168.1.1).

Each octet can range from 0 to 255, allowing for approximately 4.3 billion unique addresses (2^32).

Example: The address 192.0.2.1 indicates a specific device on a network.

IPv6:

Developed to address IPv4 exhaustion, IPv6 uses 128-bit addresses, represented as eight groups of four hexadecimal digits (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).

Provides an exponentially larger address space, accommodating trillions of devices.

Uses features like auto-configuration, better routing efficiency, and built-in security.

Public vs. Private IP Addresses:

Public IP Addresses: Assigned to devices that are directly accessible over the internet. They are unique across the entire internet.

Private IP Addresses: Used within local networks (e.g., homes, businesses) and not routable on the internet. Examples include 192.168.x.x and 10.x.x.x.

Dynamic vs. Static IP Addresses:

Dynamic IP Addresses: Assigned by a DHCP (Dynamic Host Configuration Protocol) server, which can change over time. Most home networks use dynamic IPs.

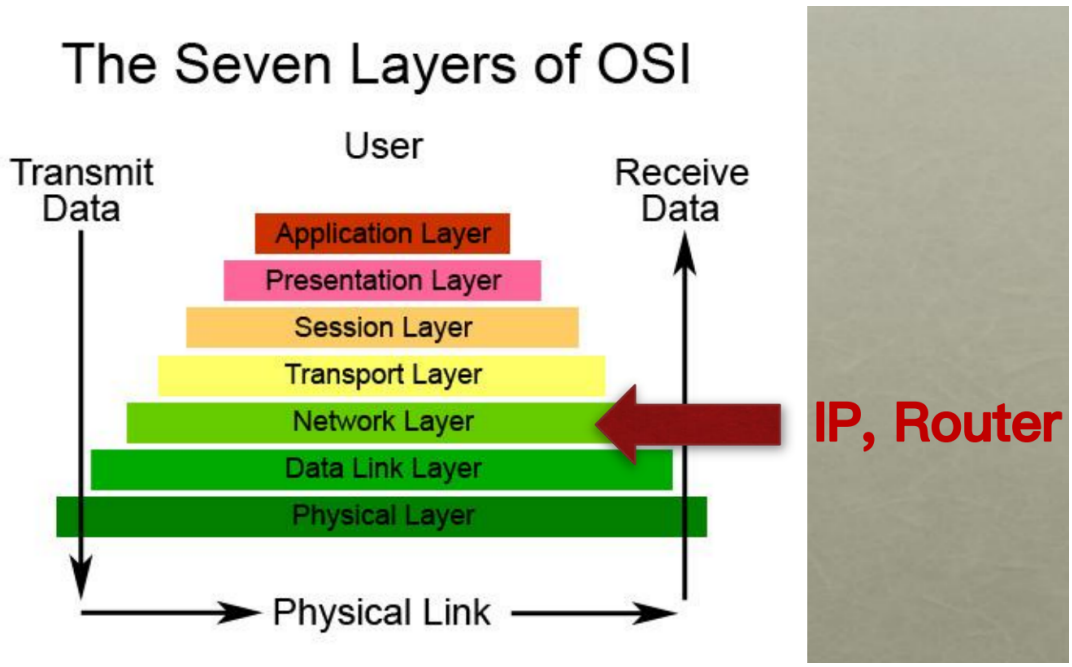
Static IP Addresses: Manually assigned and do not change, used for servers or devices that need a consistent address.

An IP (Internet Protocol) address is a unique identifier for a device on a network.

3. IP Addresses and Internet Routing Protocols

IP Addresses

Definition: An IP (Internet Protocol) address is a unique numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. It serves two main functions: identifying the host or network interface and providing the location of the device in the network.



Routers

What do routers do?

Routers forward data packets between different networks, determining the optimal path for data to travel based on the recipient's IP address.

---

4. Bandwidth and Latency

Bandwidth:

The amount of data that can be transferred over a network in a given period of time.

Measured in bits per second (bps), kilobits per second (Kbps), or megabits per second (Mbps).

Example: An internet connection with 56 Kbps bandwidth can transfer 56,000 bits per second.

Latency:

The time it takes for a data packet to travel from its source to its destination and back (also called round-trip latency).

Measured in milliseconds (ms).

Lower latency means quicker data transmission.

---

5. Data Transmission and Packets

Data Packets:

Data on the internet is broken down into smaller units called packets. Each packet contains a portion of the message, plus information about the sender, receiver, and the sequence in which it should be reassembled.

Packet Routing:

Routers send packets across the internet using the most efficient route possible, based on network traffic and availability.

---

6. Redundancy and Fault Tolerance

Redundancy

What is Redundancy?

Redundancy refers to the presence of multiple pathways for data transmission on the internet.

This ensures that if one path fails or is blocked, data can still reach its destination via alternative routes.

Fault Tolerance

What is a Fault-Tolerant System?

A fault-tolerant system continues to function even when some components fail.

The internet is fault-tolerant due to its redundant paths, which prevent single points of failure from disrupting communication.

---

7. Internet Security

Encryption

Encryption: The process of encoding data so that only authorized parties can read it. It's essential for secure communication on the internet.

Symmetric Encryption: Uses the same key to encrypt and decrypt data.

Asymmetric Encryption: Uses a pair of keys – one public, one private – for encryption and decryption. Data encrypted with the public key can only be decrypted by the private key, and vice versa.

Cybersecurity Threats

DDoS Attacks (Distributed Denial-of-Service): Attackers flood a server with excessive traffic, making it unavailable to legitimate users.

Phishing: Fraud attempts to obtain sensitive information by disguising as trustworthy entities, often through email or fake websites.

For MORE INFORMATION ON PYTHON CODING PLEASE REFER TO LAB1-3LECTURE IN THE GROUP CHATS