Chapter 1

Prima Parte

1.1 Rappresentazione dei numeri

I numeri possono essere rappresentati in qualsiasi base, noi utilizziamo la base 10 come conseguenza del numero delle nostre dita.
I **calcolatori** utilizzano la base 2, ovvero il binario, che può facilmente essere ricondotta alla condizione di uno stato elettrico o **positivo (1)** o **negativo (0)**
Per la rappresentazione di un numero in qualsiasi base:

Definizione 1:
La sequenza di k cifre:

$$d_k \cdot d_{k-1} \cdot \cdots \cdot d_1 \cdot d_0 \tag{1.1}$$

E questa sequenza la moltiplichiamo per la base scelta:

$$d_k \times b^k \cdot d_{k-1} \times b^{k-1} \cdot \cdots \cdot d_1 \times b^1 \cdot d_0 \times b^0 \tag{1.2}$$

*dove **b** è la base da noi scelta.*

Definizione 2 (Numero di cifre in una base N)**:**
In una qualsiasi base N il numero di cifre equivale a:

$$cifre = N-1, N-2, \ldots, 1, 0. \tag{1.3}$$

1.1.1 Notazione

Definizione 3 (BIT)**:**
***Bit** = binary digit, uno dei due simboli (0, 1) del sistema numerico binario. Esso è l'unità elementare dell'informazione trattata da un elaboratore.*
Numeri di 8, 16, 32 bit equivale in base 10 a parlare di numeri a 3, 4, 5, ... cifre

Definizione 4 (BYTE)**:**
***Byte** = 8 bit, è una sequenza di bit, convenzionalmente l'unità di misura delle capacità di una memoria.*
Può assumere $2^8 = 256(0 - 255)$ *possibili valori*

Definizione 5 (Parola)**:**
Word/Parola *= corrisponde a 16, 32 o 64 bit in base al tipo di IS (Instruction Set), essa è l'unità più piccola di informazione su cui un elaboratore può intervenire.*

Nome	Simbolo	Multiplo in base 10	Multiplo in base 2
chilobyte	kB	10^3	2^{10}
megabyte	MB	10^6	2^{20}
gigabyte	GB	10^9	2^{30}
terabyte	TB	10^{12}	2^{40}
petabyte	PB	10^{15}	2^{50}

Convenzionalmente si utlizzano come unità di misura:

- il B(yte) per la capacità di una memoria
- il b(it)/s per la velocità di trasmissione di dati.

1.1.2 Binario

Con la base 2 abbiamo le cifre dallo 0 allo 1.
Per la definizione precedente la rappresentazione sarà:

$$d_k \times 2^k \cdot d_{k-1} \times 2^{k-1} \cdot \cdots \cdot d_1 \times 2^1 \cdot d_0 \times 2^0 \tag{1.4}$$

Definizione 6 (Valore minimo e massimo)**:**
Il valore minmo e massimo di un numero di n cifre è:

- ***Valore minimo*** $= 000000 \ldots 00(n\ times) = 0$
- ***Valore massimo*** $=111111 \ldots 11(n\ times) = 2^n - 1$

$$2^{n-1} + 2^{n-2} + \cdots + 2^2 + 2^1 + 2^0 = 2^n - 1 \tag{1.5}$$

Esempio 1.

$$n = 3 \implies 111 = 2^2 + 2^1 + 2^0 = 7 = 2^3 - 1 = 8 - 1 \tag{1.6}$$

1.1.3 Decimale

Nella rappresentazione decimale abbiamo le cifre dallo 0 al 9.
Un qualsiasi numero in base decimale si può rappresentare come:

$$d_k \times 10^k \cdot d_{k-1} \times 10^{k-1} \cdot \cdots \cdot d_1 \times 10^1 \cdot d_0 \times 10^0 \tag{1.7}$$

Binario	Esadecimale
0000	0
0001	1
0010	2
0011	3
0100	4
0101	5
0110	6
0111	7
1000	8
1001	9

1.1.4 Ottale

Nella rappresentazione ottale si hanno le cifre dallo 0 al 7.
Questa base viene utilizzata perchè essendo un multiplo di 2 si possono facilmente convertire numeri ottali in binario:
Con 3 cifre si possono rappresentare 8 bit. In questo modo si possono avere numeri più facilmente maneggiabili da umani, rispetto a lunge stringhe di 0 o 1.

Binario	Ottale
0000	0
0001	1
0010	2
0011	3
0100	4
0101	5
0110	6
0111	7

1.1.5 Esadecimale

Nella rappresentazione esadecimale si hanno 15 cifre: dallo 0, ..., 9, A, ..., F.
Un simbolo (cifra) in questa base rappresenta 4 cifre binarie (4 bit).
Con 4 cifre esadecimali si possono rappresentare 16 bit.

Binario	Esadecimale
0000	0
0001	1
0010	2
0011	3
0100	4
0101	5
0110	6
0111	7
1000	8
1001	9
1010	A
1011	B
1100	C
1101	D
1110	E
1111	F

1.1.6 Algebra di Boole

Essa viene utillizzata per la specifica di funzioni logiche.
Una qualsiasi variabile può assumere 2 valori: **vero** o **falso**

Definizione 7 (Operazoini logiche di base)**:**

$$\begin{aligned} A\ AND\ B &= A \cdot B \\ A\ OR\ B &= A + B \\ NOT\ A &= \overline{A} \end{aligned} \tag{1.8}$$

A	B	$A\ AND\ B$	$A\ OR\ B$	$NOT\ A$
0	*0*	*0*	*0*	*1*
0	*1*	*0*	*1*	*1*
1	*0*	*0*	*1*	*0*
1	*1*	*1*	*1*	*0*

Si indica con: $\oplus = xor$, è l'or esclusivo, esso è vero solo quando una delle due variabili è vera, non quando lo sono entrambe.
$\overline{A \cdot B} = nand$, l'opposto dell'AND classico
Grazie a XOR e NAND si possono rappresentare tutte le altre funzioni logiche attraverso delle combinazioni di questi due.

A	B	$(\overline{A})$	A · B	A + B	$\overline{A \cdot B}$	$\overline{A + B}$	A ⊕ B
0	0	1	0	0	1	1	0
0	1	1	0	1	1	0	1
1	0	0	0	1	1	0	1
1	1	0	1	1	0	0	0

1.2 APPROACH

There's a difference between
Computer architecture and **Computer organization**.

- C.Architecture = attributes of a system visible to a programmer.
  ISA = Instruction set architecture, is a synonym of C.A.
- C.Organization = operational units and their interconnections that realize the architectural specifications. Examples:
  - instruction set
  - number of bits used to represent various data types
  - I/O mechanisms and techniques for adressing memory

1.2.1 Structure and function

A modern computer is a hierarchical system, and is a set of interrelated subsytems. These have, in turn, subsystems of their own until we reach the lowest level of subsystems. There's a huge difference between:

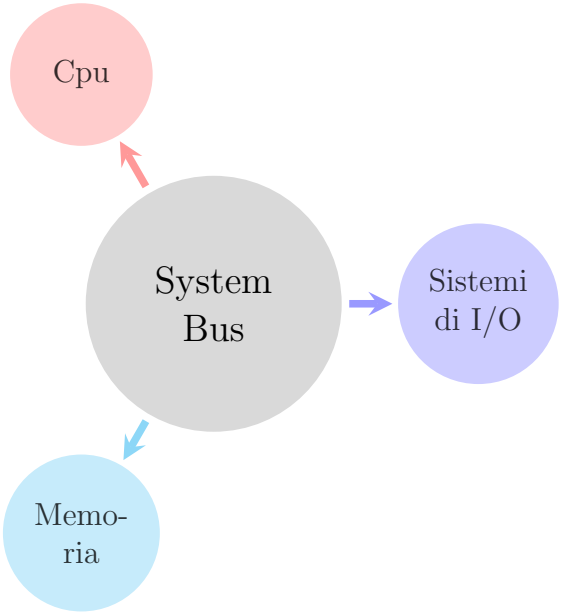
- **structure** the way components are interrelated
- **function** the operation of each individual

The way that is considered most efficient and the clearest approach for describing pc components is:**TOP-DOWN**

1.3 Componenti principali

Le componenti principali di un elaboratore sono:

- CPU
- Memoria
- Sistemi di I/O
- Interconnessioni (system bus)



Definizione 8 (Architettura di Von Neumann)**:**
Secondo questo tipo di architettura, un elaboratore è composto di questi principali componenti:

- *dati e istruzioni in memoria*
- *memoria accessibile per indirizzo*
- *esecuzione sequenziale delle istruzioni*

Definizione 9 (Programma cablato)**:**
Consiste nel costruire i componenti logici in modo tale che il risultato sia quello voluto e non può essere modificato in seguito.
Vuol dire "programmare" a livello hardware, ovvero con le componenti fisiche.
Non è un sistema flessibile, esegue solo operazioni predeterminate.

Definizione 10 (Programma)**:**
Un programma è una sequenza di passi
Ogni passo corrsiponde ad un'operazionie logica.
Ogni operazione determina un diverso insieme di segnali di controllo.

Definizione 11 (Programmazione software)**:**
Nasce con Von Neumann, si parte da un hardware generico, si ha una parte che preleva il codice di una istruzione, è generale: L'hardware di cui parliamo si dice ***general purpose****, utile a vari scopi. Si hanno poi dei segnali di controllo corrispondenti.*
Questo sistema è molto più flessibile di quello "cablato".
La CPU assume delle funzioni diverse ovvero:

- *interprete delle istruzioni*
- *generico modulo per operazioni aritmetico logiche = ALU*

I segnali di controllo sono necessari per far eseguire al giusto modulo la giusta operazione: ALU
ALU prende segnali di controllo ed esegue le istruzioni codificate
In questo sistema si ha la codifica delle istruzioni e la decodifica delle istruzioni.

Definizione 12 (Memoria principale nell'architettura di Von Neumann)**:**
Si ha la possibilità di salti oltre che all'esecuzione sequenziale(in serie)
Per esempio con le operazioni che richiedono accesso a più dati in memoria nello stesso momento.
Inoltre essa ha il compito di immaggazzinare dati e istruzioni

Esempio 2.
Somma con 2 numeri in locazione di memoria diverse

1.4 CPU

Essa non deve solo eseguire istruzioni ma anche gestire dei segnali di controllo e getstire delle risorse.
Composta da Vari componenti principali:

- **EU** = execution unit = alu
- **IR** = instruction register, registro che contiene l'istruziuone da eseguire successivamente a quella nel PC.
- **PC** = program counter, puntatore all'istruzione indirizzo dell'istruzione da eseguire presente nella memoria.
- **MAR** = memory address register, registro di interfaccia con il bus di sistema, contiene solo registri
- **MBR** = memory buffer register, contiene solo dati.
  Il MAR e il MBR mantengono le infromazioni fino a che non è disponibile il bus di sistema per essere impiegato.
  - in caso di lettura raccolgono il dato dal bus.
  - in caso di scrittura contengono il dato.
- **I/O AR** indirizzo periferica con cui scambiare dati, specificare periferica
- **I/O BR** raccolta dati

Quando si ha un salto nell'esecuzione delle istruzioni incrementa l'indirizzo del PC
Inoltre è presente un buffer nel modulo I/O: è una memoria interna al sistema di input output, esso serve perchè la CPU invia dati troppo velocemente rispetto ed esso non può riceverli alla stessa velocità, per questo il buffer dell'I/O, mantiene in memoria i dati inviati dalla più veloce CPU

1.4.1 Funzionamento CPU

- **Fetch**: reperimento, prelievo dell'istruzione dalla memoria
- **Execute**: esecuzione dell'istruzione prelevata dalla memoria

Il registro **PC** contiene l'indirizzo di memoria della cella di Memoria contenente l'istruzione da eseguire. Quando si ha un prelievo di istruzioni dalla memoria, si ha un incremento del PC. L'istruzione prelevata viene messa in IR poi viene eseguita.

1.4.2 Tipi di Operazioni

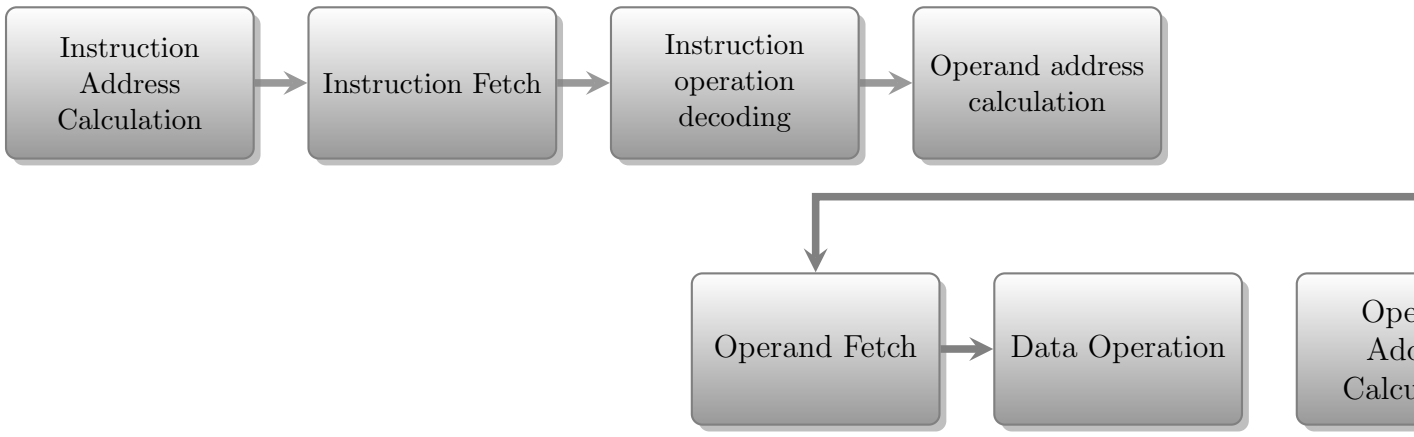
1. Processore-memoria: trasferimento dati dalla CPU alla Memoria R/W
2. Processore-I/O: trasferimento dati da CPU a I/O R/W
3. Elaborazione dati: operazioni logiche e aritmetiche sui dati operazioni della ALU
4. Controllo: può alterare la sequenza delle istruzioni, per esempio il salto

Esempio 3.
Parola = 16bit
Istruzione = 16bit
Codici operativi = 4 bit a sinistra = 2^4 combinazioni = 16

- 0001 carica in AC (accumulatore) una cella di M
- 0010 scrive in M il contenuto di AC
- 0101 somma una cella di M ad AC

1.4.3 Ciclo di esecuzione

1. Instruction Address Calculation
2. Instruction Fetch
3. Instruction operation decoding
4. Operand address calculation
5. Operand Fetch
6. Data operation
7. Operand address calculation
8. Operand Store



Per l'esecuzione di una singola operazione, bisogna prima eseguire una serie di altri sotto-compiti, che devono essere ben eseguiti.
Per questo è essenziale **l'unità di controllo**, per accertarsi che ogni operazione venga eseguita correttamente e nel giusto ordine.
La CPU può eseguire **più operazioni** momentaneamente, mantenendo ogni sua parte attiva , breve introduzione al concetto di pipeline

1.4.4 Interruzioni

Il meccansimo tramite il quale dei moduli possono interrompere la normale di sequenza di esecuzione.
Il ciclo di esecuzione con interruzioni è differente: al **termine** di un ciclo si ha il controllo delle interruzioni,

- se ce ne sono, esse vengono risolte
- se non ce ne sono, il ciclo ricomincia

Tipi di interruzioni:

- Program, overflow, divisione per zero
- Timer, da un timer inerno alla CPU
- I/O, termine di un'operazione di I/O
- Guasto Hardware

Si interrompe per

- efficienza elaborazione

Ciclo interruzione:

- viene aggiunto al ciclo di esecuzione
- la cpu controlla (fetch) le interruzioni pendenti
- se non ce ne sono, prende la prossima istruzione
- se ce ne sono:

- sospende esecuzione
- salva contesto
- imposta il pc all'indirizzo di inizio del programma di gestione
- esegue il programma di gestione dell'hardware
- rimette il contesto al suo posto e continua il programma interrotto

Lunghezza di attesa:

- **breve attesa**, tempo di operazione di I/O minore del tempo tra due istruzione WRITE
- **lunga attesa**,

Interruzioni multiple

In caso di **interruzioni multiple**: esistono vari livelli di interruzione e differenti tipi di politica di gestione.
Esistono interruzioni di alto livello e basso livello, a seconda dell'importanza che hanno per il funzionamento del sistema.
Politiche di interruzione:

- Disabilitare le interruzioni:
  - La CPU **ignora** le altre interruzioni e gestisce la prima e "maschera" le altre
  - Le interruzioni rimangono **pendenti**
  - vengono gestite nell'**ordine** in cui arrivano
- Definire le priorità
  - Interruzioni di bassa priorità vengono interrotte quando si presentano quelle di alta priorità
  - Quando è stata gestita la priorità di alto livello viene maneggiata quella di basso livello
  - Si hanno delle interruzioni **annidate**

1.5 Interconnessioni

Tutti i componenti **devono** essere connessi
Esistono vari tipi di connessioni per vari tipi di componenti, il bus collega:

- CPU
- Memoria
- I/O

Composto da 50 a qualche centinaio di linee

1.5.1 Bus

Tutti i dispostivi sono collegati dal bus di sistema
Il bus:

1. collega **2 o più** dispositivi
2. mezzo trasmissione condiviso
3. un segnale trasmesso ad un bus è disponibile a tutti i dispositivi
4. arbitro bus: solo un dispostivo alla volta può trasmettere
5. varie linee di comunicazione (trasmettono uno 0 o un 1)
6. varie linee trasmettono in parallelo numeri binari. Un bus da 8 bit trasmette un dato di 8 bit

Solitamente l'ampiezza del bus corrisponde ad un multiplo della parola.
Tipi di bus:

1. Bus di sistema:
   - connette cpu, i/o, M
   - da 50 a qualche centinaio di linee
   - 3 gruppi di linee
     (a) bus dati
     (b) indirizzi
     (c) controllo
2. Bus dati:
   - trasporta dati o istruzioni
   - ampiezza –> efficienza del sistema
     – con poche linee –> maggiori accessi in memoria
3. Bus indirizzi:
   - indica sorgente o destinazione dati
   - l'ampiezza determina la massima quantità di M indirizzabile

     Esempio 4.
     Architettura a 64 bit = $2^{64} - 1$ indirizzi
     Il bus deve essere di almeno 64 bit.

   - deve essere di almeno 1 parola
4. Bus controllo:
   Per controllare accesso e uso di:
   - **linee dati**
   - **indirizzi**
     (a) M write

(b) M read
(c) richiesta bus
(d) bus grant
(e) interrupt request
(f) clock

1.5.2 Uso del bus

Con modulo intendiamo una generica componente del computer.
se un modulo vuole inviare dati ad un altro:

- bus grant
- data transfer

se un module vuole ricevere dati da un altro:

- bus grant
- trasferire una richiesta all'altro modulo sulle linee di controllo
- attendere invio dati

1.5.3 Bus singoli e multipli

- singolo bus = ritardo e congestione
- vari bus = risoluzione problema

Esempio di Bus multiplo:

- **connessione punto a punto** fra CPU e cache, il che rende il trasferimento dei dati molto più veloce ed efficiente.

- **Bus di espansione**, si interfaccia con i dispositivi I/O
- **Bus ad alta velocità**, si interfaccia con i dispositivi I/O e fornisce una trasmissione di dati più rapida
- **Bus di sistema**, fra cache e Memoria principale.

1.5.4 Temporizzazione

Coordinazione degli eventi su un bus

- Asincrona
  - più complessa da implementare
- Sincrona
  - clock determined events
  - single clock line, with an alternate sequence of 0 and 1, with equal length
  - single 1-0 sequence is a clock cicle
  - every device connected to the bus can read the clock line
  - every event starts at the beginning of a clock cycle

QPI

Interconnessione Punto a Punto, con l'aumentare della velocità dei processori è sempre più frequenta una distribuzione di dati densa e veloce.
Un bus condiviso però rallenta la comunicazione del processore (bottleneck) , per questo si adottano delle connessioni punto a punto.

- Connessioni dirette multiple:
  più componenti del sistema godono di connessioni dirette a coppie con altri componenti.
- Architettura di protocollo a strati
- Trassferimento Dati a pacchetto:
  i dati non sono inviati come flussi di dati non elaborato ma come una sequenza di pacchetti, essi includono intestazioni di controllo e codici di correzione dell'errore.

Livelli di QPI:

- **fisico**
  la parte hardware, l'unità di trasferimento è di 20 bit (Phit) , tutto è sincronizzato da un clock.
- **Link**
  trasmissione affidabile del controllo del flusso, l'unità di trasferimento è di 80 bit (Flit).
  Protocollo con pacchetti da 72 (dati) + 8 (codice di correzione errore) bit.
  - Controllo del flusso:
    il mittente non può inviare più dati di quelli che il destinatario può ricevere.
  - Controllo dell'erroreç 8 bit per rilevare errori di trasmissione sugli altri 72 bit.
    In caso di errore il mittente deve re-inviare il pacchetto errato.
- **Routing**
  Struttura per dirigere i pacchetti attraverso essa. Determina il percorso che un pacchetto deve seguire.
  Supportato da tabelle di instradamento:
  - definite da software di basso livello che contiene delle istruzioni
  - descrizione percorso che un pacchetto può seguire
  - utile in sistemi di maggiori dimensione
- **Protocollo**
  Insieme di regole ad alto livello per lo scambio di pacchetti. Un pacchetto è un numero intero di Flits. Il contenuto di un pacchetto è flessibile, per gestire esigenze diverse.
  Supporta il protocollo di coerenza della cache, per garantire coerenza fra i contenuti della cache dei core e la memoria principale

1.6 Memorie

Caratteristiche principali della memoria:

- Locazione: processore (cache), interna (principale RAM), esterna (secondaria)
- Capacità: dimensione parola (dipende dall 'architettura), numero di parole
- Unità di trasferimento: parola, fra cache e RAM in blocco (insieme contiguo di parole)
- Metodo di accesso:
  - sequenziale: accedere prima a tutte le informazioni che vengono prima: lento. Utilizzato nei nastri magnetici, backup sistemi.
  - diretto, organizzata in gruppi, accesso sequenziale ai gruppi. accesso diretto ad un insieme di informazioni. HDD
  - casuale, accesso diretto a quella locazione di memoria, non importa dove si trova la locazione di memoria dell'informazione. RAM
  - associativo, informazione non indviduata da indirizzo, ma da una parte dell'informazione. CACHE
- Prestazioni: tempo di accesso, ciclo e velocità di trasferimento
- Modello fisico:
  - semiconduttore (ROM)
  - magnetico, campi magnetici (HDD)
  - ottico, laser ottico (CD)
  - magnetico-ottico
- Caratteristiche fisiche:
  - volatile (cache, quando termina il flusso di corrente elettrica i dati vengono cancellati)
  - non volatile (hdd, i dati vegnono memorizzati permanentemente quando si spegne il computer)
  - riscrivibile (RAM, HDD, cache)
  - non riscrivibile (ROM, read only memory).
- Organizzazione, se suddivisa in un singolo chip oppure vari, più o meno moduli.

Generalmente all'aumentare del costo della memoria aumenta la sua velocità ma diminuisce la sua ampiezza.
In ordine decrescente per velocità, costo e crescente per ampiezza:

- Registro (1 parola) 16 - 64 bit
- Cache (1 indirizzo)
- SRAM
- DRAM (8gb - 64gb)
- SSD (1TB - 8TB)

- HDD (16TB-24TB)
- CD - DVD-ROM
- Nastro (vari PB)

L'aumento di prestazioni delle CPU si deve a migliorie tecnologiche e architetturali, mentre quello delle memorie **solo** ad avanzamenti tecnologici.
Proprieta' dei programmi:

- Statiche, dal file sorgente
- Dinamiche, dall'esecuzione
  - Linearita' dei riferimenti, spesso consecutivi
  - Localita' dei riferimenti, indirizzi contigui sono piu' probabili

Definizione 13 (Congettura 90/10)**:**
Un programma impiega di solito il 90% del suo tempo di esecuzione alle prese con un numero di istruzioni pari a circa il 10% di tutte quelle che le compongono.

1.6.1 Gerarchia di memoria

Tutte le locazioni di memoria sono suddivise in blocchi.

Conviene organizzare la memoria in vari livelli gerarchici:

- Cache la più veloce e suddivisa in diversi livelli
  - L1 cache:
    molto veloce e molto costosa, per i dati ad accesso probabile
    es. 10% di cui parlavamo prima
  - L2 cache, più capiente ma meno veloce della L1.
  - L3 cache, più capiente ma meno veloce della L2
- Ram, più lenta della cache ma più capiente ed economica

La memoria Ram è composta da:

1. indirizzo di memoria
2. blocco di memoria

Memoria a livelli:

1. Livello inferiore, supporti con capacità più alti, piu' lenti, meno costosi
2. A livelli piu' alti diventano progressivamente piu' veloci, piu' costosi e meno capienti.

La CPU usa il livello piu' alto. Ogni livello inferiore contiene tutti i dati presenti ai livelli superiori.

trasferimento dati

I dati vengono scambiati sotto forma di WORD/PAROLE:

- CPU - Cache: scambio di PAROLE
- CACHE - MEMORIA P. scambio di BLOCCHI (multiplo di PAROLE)

La memoria lavora efficientemente se la CPU trova il dato cercato nella CACHE. Avendo piu' livelli di cache si ha una maggiore probabilità di trovare questo dato.

Il numero di parole in un blocco è una potenza di 2.
Una parola è composta da 4 byte, possiamo identificare i primi 14 bit come "indirizo" del bit, mentre i restanti 2 come identificativi del bit.

1.6.2 Cache

Un indirizzo di linea di cache e' costituito generalmente da:

1. Etichetta (tag), indirizzo del blocco nella memoria principale.
2. Blocco di K parole

Un blocco di memoria richiesto dalla CPU può essere presente **hit** o non presente **miss** in memoria. (generalmente è presente).
Per guadagnare efficienza prestazionale un **hit** deve essere molto probabile ($> 90\%$), se fosse minore di questa percentuale non avrebbe senso utilizzare quella struttura di memoria.
Un **miss** avvia una procedura di scambio di dati con un livello inferiore.
Una linea di cache può memorizzare diversi blocchi diversi, si usano i bit piu' a destra per identificare la parola all'interno della linea e i bit piu' a sinistra qual'e' la linea di cache per identificare il blocco.

Definizione 14 (Organizzazione)**:**
La memoria principale e' suddivisa in blocchi logici
La cache e' suddivisa in un multiplo di blocchi.

Definizione 15 (Tempo medio di Accesso)**:**
T_a*: Tempo medio di accesso ad un dato in memoria cache*

$$T_a \ = \ T_h \times P_h + T_m(1 - P_h) \tag{1.9}$$

T_h*: tempo di accesso ad un dato presnte in cache* T_m*: tempo medio di accesso ad un dato* ***non*** *in cache (dimensione blocco)* P_h*: probabilità di hit*

Tecnica generale

1. Suddivisione della memoria centrale in blocchi logici
2. dimensionamento della cache in multiplo di blocchi
3. ogni indirizzo emesso dalla cpu

- hit $\iff$ il dato viene fornito immediatamente alla cpu, (sotto forma di parola)
- miss, il dato viene fornito sotto forma di blocco
  (a) la cache richiede il dato al livello inferiore (memoria principale RAM)
  (b) viene posto in cache
  (c) viene fornito alla cpu

Definizione 16 (**associazione diretta / direct mapping**)**:**
Ogni blocco del livello ineriore può essere allocato solo in una specifica posizione ***linea/slot*** *del livello superiore*

1. ***ILS*** *= indirizzo di livello superiore*
2. ***ILI*** *= indirizzo di livello inferiore*
3. *$ILS = ILI \bmod N$, divisione con resto intero*

1. *vantaggi*
   - *semplicità traduzione indirizzo ILI a ILS*
   - *determinazione velocità hit o miss*
2. *svantaggi*
   - *necessità di contraddistinguere blocco in ILS*
   - *swap frequenti per accesso a dati di blocchi adiacenti,*
     il primo blocco di ogni insieme avrà la stessa linea di cache, quindi solo uno di questi puo' essere in cache

Definizione 17 (**associazione completa / fully associative**)**:**
Ogni blocco del livello inferiore può essere posto in qualunque posizione del livello superiore. Ad una cache di N blocchi viene associata una tabella di N posizioni contenenti il numero di blocco effettivo (tag)

- *vantaggi: massima efficienza di allocazione*
- *molto tempo per la corrispondenza ILS-ILI e della verifica hit/miss*
- *molto costoso dal punto di vista hardware e scarsa possibilità di hit*
- *difficile identificazione di hit o miss*

Definizione 18 (**associazinone a N-gruppi / N-way set associative**)**:**
Ogni blocco di un certo insieme di blocchi del livello inferiore può essere allocato liberamente in uno specifico gruppo di blocchi del livello superiore

Esempio 5.
Per una cache di 32 linee con un N equivalente a 2, ogni gruppo avrà 16 linee.
Ci sono 16 gruppi da 2 linee e per ogni coppia avremo un blocco di una determinata posizione di qualunque insieme.

Questo tipo di associazione è una via di mezzo fra gli altri due tipi. La cache composta da R gruppi di N posizioni di blocco, si affiancano R tabelle di N elementi contenenti i tag.
Per ottenere facilmente il numero di linee basta semplicemente fare la moltiplicazione

$$Numero\ di\ linee\ della\ cache = N \times R \tag{1.10}$$

Ha una buona efficienza di allocazione, nonstante abbia una certa complessità, e prende i due punti di forza degli altri due tipi:

- *uso efficiente delle linee di cache*
- *facile determinazione di hit o miss*

Non e' necessario avere un grande numero di N per raggiungere il massimo dell'efficienza1

1.6.3 Politiche di rimpiazzo dei blocchi

Quando si ha un miss, come si decide quale blocco della cache dobbiamo rimpiazzare?
Nell'associazione diretta non ci si pone questo problema, perchè ogni linea della cache corrisponde un blocco della memoria centrale.

1. *casuale*, viene occupato lo spazio omogeneamente, facile implementazione
2. *First-In-First-Out(FIFO)*, il blocco rimasto più a lungo in cache, complicata implementazione
3. *Least Frequently Used(LFU)*, il blocco con meno accessi, complicata implementazione hardware
4. *Least Recently Used(LRU)*, il blocco con l'accesso più distante, per preservare quelli accessi più recentemente, implementazione difficile.

A minor quantità di cache si hanno migliori prestazioni con il rimpiazzo LRU.
Questo e' il metodo piu' gettonato, e ad aumentare il livello di cache è sempre meno significativo il miglioramento offerto da queste tecnologie.
La scrittura dati determina incoerenza tra il blocco in cache e quello nei livelli inferiori

Definizione 19:
write through:

1. *scrittura contemporanea in cache e livello inferiore*
2. *aumento traffico per frequenti scritture nel medesimo blocco, dati coerenti fra blocchi*
3. *si ricorre a buffer asincroni verso la memoria, a causa di momenti di congestione del bus.*

La memoria contiene **istruzioni** e **dati** e solo il 50% delle operazioni sui dati sono scritture.

Definizione 20:
write back:

1. *scrittura in memoria inferiore differita al rimpiazzo del blocco di cache corrisp.*
2. *ridotto numero di modifiche nella memoria principale*

3. *occore ricordare operazioni di scrittura nel blocco*
4. *ottimizzazione del traffico tra livelli, riduzione congestione bus*
5. *periodi di incoerenza*

Occore ricordare che tra memoria centrale (RAM) e cache si passano **BLOCCHI** e non **PAROLE**.

Esempio 6 (scenario problematico).
- più dispositivi connessi allo stesso bus con cache locale
- memoria centrale condivisa

Nessun tipo di "write" (through, back) può assicurare coerenza.

Possibili soluzioni

- **monitoraggio del bus con write through**, controllori intercettano modifiche locazioni condivise
- **trasparenza hardware**, hardware aggiuntivo: modifica a RAM = modifica a cache
- **memoria non cacheable**, solo una porzione è condivisa e non cacheable

Cosa comporta la modifica di dati in una cache?

- invalida quella parola corrispondente nella memoria centrale
- invalida la parola nelle altre cache che la contengono
  per esempio in un sistema con CPU multi-core

Estendiamo il discorso alla memoria swap e RAM:
Quello che cambia e' che al livello cache-RAM e' tutto basato su un livello logico, mentre nell'altro caso si parla di un livello fisico fra RAM e memoria swap dei dispositivi di archiviazione eseterna.
Le problematiche che si incontreranno saranno le stesse: capienza RAM piena, politiche di rimpiazzo, modalita' di scrittura.
I blocchi diventano pagine di un programma.

Cache logica e fisica

Possiamo avere due tipi di Cache:

- Logica, riceve un indirizzo logico ma ad ogni cambiamento di contesto deve essere svuotata, conveniente se si prevede un utilizzo in un contesto con poche interruzioni
- Fisica, riceve un indirizzo fisico deve attendere la traduzione dell'indirizzo da logico a fisico, non deve essere svuotata ad ogni cambiamento di contesto, conveniente in un contesto con molte interruzioni

La cache deve essere svuotata ad ogni cambiamento di contesto, altrimenti non puo' funzionare bene.

Il problema dei miss

Esistono vari tipi di miss:

- di primo accesso, inevitabile non riducibile
- per capacità insufficiente, quando la cache non può contenere altri blocchi
- per conflitto, dipende dal tipo di associazione, quando vari blocchi possono corrispondere allo stesso gruppo

Soluzioni classiche:

- Maggior dimensione di blocco, aumento di miss, aumento linee utilizzo piu' efficiente dello spazio
- Maggiore associativita', incremento del tempo di localizzazione di un gruppo, soggetto alla regoal 2:1

Altre soluzioni:

- multilivello cache, fino a 3 livelli
- separazione cache dati / cache istruzioni
- ottimizzazione degli accessi mediante compilatori (C)

tipi di memorie a semiconduttore

Tipo	Categoria	Cancellamento	Mecc. scrittura	Volatile
RAM	read-write	elettric. byte-level	elettric.	si
ROM	read-only	non possibile	maschere	no
PROM	read-only	non possibile	elettric.	no
EPROM	read-mostly	luce UV, chip-level	elettric.	no
EEPROM	read-mostly	elettric. byte-level	elettric.	no
Memoria Flash	read-mostly	elettric. block-level	elettric.	no

Si dice di una memoria che e' volatile o no quando: se manca l'alimentazione l'intero contenuto della memoria si cancella.

Definizione 21 (DRAM)**:**
Dynamic RAM =

- *bit memorizzati in condensatori*
- *decadimento cariche con tempo*
- *refresh cariche, durante alimentazione*
- *semplice costruzione*

- *1 condensatore = 1 bit*
- *meno costose*
- *circuito per refresh*
- *meno veloci della SRAM*
- *usate nella RAM*
- *operazione analogica, la carica determina il valore (0 o 1)*

Definizione 22 (SRAM)**:**
Static RAM =

- *bit memorizzati tramite porte logiche*
- *non perde la carica*
- *no refresh*
- *piu' complesso, piu' elementi per bit (6 transistor)*
- *piu' costosa*
- *no refresh*
- *piu' veloce, utilizzata nella cache*
- *digitale*

1.6.4 ROM

Una ROM:

- memorizzazione permanente (non volatile)
- memorizzano:
  - microprogrammi
  - subroutine di libreria
  - programmi di sistema
  - funzioni tabulate (logaritmi, esponenziali, etc)

1.6.5 Codice correzione errore

Tipi di errori:

- Guasto hardware, non risolvibile
- errore software, possono accadere casualmente, a causa del decadimento della materia, i danni non sono permanenti

Quando un errore viene rilevato, puo' essere corretto attraverso i codici di Hamming (quelli che vedremo)
Quando un dato viene creato assieme ad esso si crea una sua 'impronta digitale' che verra' utilizzata per comparare la validita' del dato.
Si trasmettono gli 'M' bit di dati assieme a dei 'k' bit generati da una certa funzione che creano una sorta d'impronta digitale.
Attraverso la funzione che converte gli 'M' bit nei 'k' bit si utilizza per ricostruire il dato originale e confrontarlo con l'originale o lo si utilizza per correggerlo.
Questo tipo di codice di correzione è valido quando c'è un solo errore.
La formula per determinare la quantità di bit di correzione necessari:

$$2^{k-1} \geq M + K \tag{1.11}$$

Questa quantità diminuisce drasticamente all'aumentare degli 'M' bit:

Bit dati (M)	Bit controllo (k)	% incremento
8	4	50
16	5	31,25
32	6	18,75
64	7	10,94

Quando ci sono 2 errori si riesce a corregerne uno solo e si comunica che è stato rilevato un errore ma non è correggibile.

1.6.6 Memorie esterne

Le memorie esterne si suddividono in 4 macro-categorie:

- dischi magnetici
  - RAID
  - rimovibili
- dischi SSD
- ottica
  - CD-ROM
  - CD-Recordable (CD-R)
  - CD-R/W
  - DVD
- nastri magnetici

Dischi magnetici

I dischi sono ricoperti di materiali magnetici, e le informazioni è memorizzata in un campo **magnetico**.
Venivano costruiti in alluminio, mentre ora si utilizza il vetro perchè

- la sua superficie è più uniforme, (lo rende più affidabile),
- ci sono meno difetti di superficie (e ne riduce gli errori),
- è più rigido
- la testina può essere posta più vicino al disco
- è più resistente.

Il disco è organizzato in **cerchi concentrici** di informazione (chiamati tracce), il disco ruota e la **testina** viene spostata in senso radiale verso l'interno o l'esterno del disco.
Può leggere o scrivere rilevando **campi magnetici** o inducendoli. L'orientamento di un campo magnetico si determina in base al verso con cui la corrente scorre e determina il tipo di informazione che viene passata. Dato che i campi magnetici rimangono impressi nel materiale ferroso (ossido di ferro) è un dispositivo **non-volatile**.
L'interferenza fra campi magnetici è divisa fra le tracce da dei gap.
I dati vengono memorizzati tramite una bobina conduttiva di scrittura detta **testina**.
I dati sono memorizzati in anelli o **tracce concentriche**. I dischi ruotano ad una **velocità angolare costante**, ciò vuol dire che le tracce più interne a parità di rotazione perccoronon meno strada rispetto alle tracce più esterne.
Una conseguenza di questo fenomeno e del fatto che le informazioni contenute in ogni traccia devono essere della stessa quantità di byte, implica che i campi magnetici delle tracce più interne sarannno necessariamente più compatti. La densità delle tracce non è consistente.
Le tracce si dividono in:

- Settori, la dimensione minima di un blocco coincide con un settore
- Più di un settore per blocco
- Con più dischi, le tracce nella stessa posizione costituiscono un cilindro

Per **ricercare un settore** bisogna riconoscere l'inizio della traccia e del settore. Testina sulla traccia e attendere che il settore d'interesse passi attraverso la testina. (es. treno: quando prendiamo un treno ci sono 3 scenari: il treno sta per partire, dobbiamo aspettare un po', oppure il treno è già partito e dobbiamo aspettare il prossimo. Si può fare un'analogia con la testina (noi) settore (treno)). Il **formato di un disco** è:

- Informazioni aggiuntive non disponibili all'end user
- demarca tracce e settori

Esempio 7 (Disco Winchester).
In esso si possono ottimizzare la distanza fra traccia e testina.
In particolare un settore di questo formato è composto da 600B:

- GAP 1 = 17B
- Campo ID = 7B

  - Byte di sincronizzazione = 1B
  - N° traccia = 2B
  - N° testina = 1B
  - N° settore = 1B
  - Codice correzione errore = 2B
- GAP 2 = 41B
- Campo dati = 515B
  - Byte sincronizzazione = 1B
  - Dati = 512B
  - Codice correzione errore = 2B
- GAP 3 = 20B

Caratteristiche di un dispositivo di memorizzazione esterna:

- Testina
  - Fissa (raro)
  - mobile
- Disco
  - Rimovibile
  - Fisso
- Fascia
  - singola
  - doppia
- Piatto
  - singolo
  - doppio
- Meccanismo della testina:
  - contatto (floppy)
  - distanza fissa
  - seprazione aerodinamica
    * Testine foil planano sulla superificie dei dischi sfruttando la portanza del profilo
    * Testine vicinissime alla superficie dei dischi

Prestazioni

Le prestazioni di un disco eseterno sono determinate da:

- Tempo di posizionamento (T_P) (seek time), spostamento della testina nella traccia giusta, all'incirca dai 5 ai 20ms, non molto ottimizzabile essendo uno spostamento meccanico
- Latenza rotazionale (T_L) (latency), attendere che il settore d'interesse sia sotto la testina, dipende dalla velocità di rotazione (RPM)

$$RPM = 3600 \implies RPS = 60 \implies rotazione = 16.7ms \implies T_L = 8.35ms \quad (1.12)$$

- Tempo di accesso, ($T_P + T_L$) determinato dal tempo di posizionamento e dalla latenza (seek + latency)
- Tempo di trasferimento:

$$T = \frac{b}{r \times N} \quad (1.13)$$

dove **b** = byte da trasferire, **N** = numero di byte per traccia e **r** = velocità rotazione in secondi.

RAID

Redundant Array of Independent(/Inexpensive) Disks, esistono 7 livelli (da 0 a 6) non gerarchici di dischi, si tratta di un insieme di dischi fisici visti dal sistema operativo come un singolo dispositivo logico. In questo tipo di configurazione i dati sono distribuiti sui dispositivi.

RAID 0: nessuna ridondanza, tutti i dati sono distribuiti nei dischi in *strisce* (strip), si utilizza il metodo 'round robin striping' e si ottiene una maggiore velocità sia in scrittura che in lettura.
Le strip vengono memorizzate in parallelo nei vari dischi. Una strip è un multiplo di blocchi.
C'è un'alta probabilità che i dati siano distribuiti in vari dischi e quindi che non ci sia un conflitto di risorse.

RAID 1: Mirrored, il contenuto viene replicato su più dischi, ogni dato viene copiato in un altro disco. Ogni dato viene letto e scritto in più dischi. Il vantaggio è il recupero dei dischi immediato, è necessario solamente sosituire il disco rotto con quello che ha gli stessi dati. Si ha una copia esatta di ogni disco.

RAID 2: (non commercializzato), dischi sincronizzati, in modo tale che la testina di ogni disco sia nella stessa posizione in ogni disco, si usano unità di informazione molte piccole.
Si hanno codici di correzione calcolati tra bit corrispondenti nei vari dischi. Si ha una grande ridondanza, ciò fa aumentare di molto il costo.

RAID 3: simile al raid 2, ma ha solo un disco ridondante indipendentemente dal numero di dischi nell'array. Non è necessario sapere quale dato viene a mancare ma semplicemente quale disco non è più funzionante, quindi con questo sistema si sostituisce il disco guasto direttamente. Usa un semplice bit di parità per ogni insieme corrispondente di bit, attraverso questi si ricostruisce l'informazione e ai dati presenti negli altri dischi. Si ha un'alta velocità di trasferimento. La sincronizzazione dei dischi è causa di complessità, il disco di parità diventa il 'collo di bottiglia' per le operazioni in parallelo ed è quello più facile a subire un guasto

RAID 4: Ogni disco opera indipendentemente, ottimo per alti ritmi di richieste I/O, l'informazione di parità viene memorizzata su un disco ad hoc (disco di parità). Il problema di questa configurazione è il disco di parità che diventa un 'collo di bottiglia', essendo frequentemente utilizzato è quello più probabile a subire dei problemi di malfunzionamento

RAID 5: la parità viene distribuita in dischi diversi, non si ha più il collo di bottiglia dei RAID 3&4. L'allocazione viene distribuita con il metodo 'round robin', esattamente come i dati nel RAID 0, viene utilizzato nei server di rete, uguale al RAID 4 fuorchè per il disco di parità, robustezza fino ad un disco. Per avere 'N' dischi occorre averne 'N+1'

RAID 6: Si calcola la parità tramite due metodi distinti che sono memorizzati in blocchi separati in dischi differenti. Per avere 'N' dischi occorre averne 'N+2', si ha una robustezza fino a 2 dischi, equivale al RAID 5 con il doppio della parità.

Dischi SSD

Solid State Drive, Solid perchè si basa su circuiti integrati ovvero **memorie flash** di tipo NAND
Il **floating gate**

- non attivo, non interferisce con il control gate e rappresenta bit a 1, di default è in questo stato.
- se attivo, tramite alto voltaggio intrappola elettroni che rimangono anche in assenza di alimentazione e rappresnetano bit a 0 e rende il transistor come se fosse inutilizzabile

La struttura di una memoria flash di tipo NAND è organizzata in arraya da 16 o 32 transistor collegati in serie. La bit line va a 0 solo se tutti i transistor delle corrispondenti linee della parola sono a 1 (attivi), deriva dalla funzione booleana NAND. Le letture e le scritture coinvologono l'intera parola.
I vantaggi di questi dischi sono:

- velocità, non sono coinvolte operazioni meccaniche.
- alte prestazioni di I/O e aumenta le prestazioni dei sottoinsiemi di I/O
- durata, meno suscettibile a urti e vibrazioni rispetto ai dischi magnetici
- maggiore durata, non soggetti a usura meccanica
- consumo energetico inferiore, meno energia non essendo coinvolte parti meccaniche.
- funzionalità più silenziose e fredde, minori costi energetici
- tempo di accesso e latenza inferiori oltre 10 volte rispetto a quelli degli HDD

Organizzazione di un disco SSD:

- Sistema host:
  1. per accedere ai dati, il sistema operativo richiama il software del file system, che richiama a sua volta il software del driver di I/O che fornisce l'accesso all'SSD
  2. il componente di interfaccia si riferisce all'interfaccia fisica ed elettricatra il processore host e l'SSD
- SSD:

1. Controller: fornisce l'interfacciamento a livello del dispositivo SSD e l'esecuzione del firmware
2. Indirizzamento: logica che esegue la funzione di selezione tra i componenti della memoria flash
3. Buffer/cache dati: RAM ad alta velocità per compensare velocità e aumentare il throughput dei dati
4. correzione degli errori: logica per il rilevamento e la correzione degli errori
5. Componenti della memoria flash: singoli chip flash NAND

Gli svantaggi degli SSD:

- Le performance decadono con l'uso, la dimensione di un blocco delle memorie flash all'interno degli SSD è di solito di 512kb, per poter scrivere anche solo un B bisogna portare il blocco in cache e modificare l'intero blocco riscrivendolo da capo.
  I file sono di solito salvati in pagine da 4kB quindi 128 pagine per blocco. con l'utilizzo dei file essi si frammnetano, le pagine vengono memorizztei in blocchi diversi e le prestazioni decadono.
  soluzioni: over-provisioning, vengonon tenuti certi blocchi solamente per le scritture; cancellazione delle pagine inattive; comando TRIM (avverte il dispositivo quali pagine sono state memorizzate logicamente).
- si ha un numero limitato di scritture, intorno alle 100.000, per risolvere questa limitazione, cache front-ending (ospita blocchi più riferiti, politica LRU), distribuzione scritture, gestione blocchi esauriti, RAID.

Memorizzazione Ottica

Inizialmente furono concepiti per organizzare dati audio: 650MB memorizzano più di 70 minuti audio.
Sono principalmente dischi di policarbonato rivestiti con un materiale altamente riflettente.
I dati sono memorizzati come microscopici pozzetti:

- Land
- Pit

i dati 0 e 1 vengono memorizzati come transizione da land e pit o viceversa e vengono letti tramite laser.
Si ha una densità di memorizzazione costante, infatti si ha una singola traccia organizzata a spirale e gira a velocità costante, la velocità del disco dipende dalla posizione in cui si trova.

CD-ROM

Caratteristiche:

- Audio: singola velocità
  - velocità lineare costante
  - 1.2 ms^{-1}
  - traccia a spirale lunga 5.27km

  - memorizza 4391 secondi = 73.2 minuti
- la velocità dichiarata è la massima raggiungibile che il lettore può raggiungere.
- formato dati:
  - modo 0 = campo dati vuoto
  - modo 1 = 2048 byte dati+correzione
  - modo 2 = 2336 byte dati

Accesso casuale su CD-ROM:

- difficile causa della velocità lineare costante
- spostare la testina in posizione approssimata
- configurare la giusta velocità di rotazione
- legere l'indirizzo
- altri aggiustamenti per spostarsi sul settore richiesto

Non è però efficiente come in una memoria RAM
Pro:

- Capacità, si utilizzavano come sistemi di bakcup, erano più economici degli HDD
- facili da produrre su grande scala
- rimovibile
- robusto

Contro:

- Costoso per piccole quantità
- lento per accedere ai dati
- essendo un CD-ROM è di solo lettura

1.7 Formulario

Altri tipi di memorizzazione ottica

- CD-R(ecordable)
- CD-RW
- Digital video Disk usato per riprodurre film,
  sono presenti molteplici strati,
  ha un'alta capacità di memorizzazione
  si usa tutto lo spessore del disco e inoltre si usano entrambi i lati di esso,
  il diametro del raggio laser è minore quindi si ha una maggiore densità di memoria

1.7.1 Nastro magnetico

- Accesso seriale
- lento
- molto economico
- utilizzato per backup e copia di riserva

Le informazioni possono essere memorizzate a serpentina, o possono essere scritte a blocchi