Calcolatori

Giacomo Fantoni

6 giugno 2019

Indice

Capitolo 1

La codifica del testo

Per rappresentare i caratteri da sequenze di zeri e uni si deve utilizzare una codifica che si basa sull'alfabeto anglosassone a 7 bit (128 caratteri diversi) e si chiama ASCII (American Standard Code for Information Interchange). Essendo che i byte sono composti da 8 bit il bit più significativo rimane zero e viene utilizzato in altre codifiche per caratteri addizionali. Queste nuove codifiche non sono univoche e dipendono dall' area geografica per supportare i vari alfabeti. Per sopperire a questo problema si utilizzano altre codifiche univoche come unicode a 32 bit, UTf-32, UTF-16 o UTF-8, compatibile con ASCII

Capitolo 2

Reti logiche

I computer moderni sono realizzati tramite circuiti elettronici che si basano su due livelli fondamentali: alto o asserito (1), associato alla tensione di alimentazione Vdd e bassso o negato (0) associato alla massa (con tensione 0), gli altri livelli di tensione non sono significativi e assunti solo in fase transitoria.

2.1 Porte logiche

Sono circuiti che trasformano valori logici in ingresso in altri valori logici in uscita. Si dividono in;

1. Combinatorie, con una relazione funzionale tra ingresso e uscita, senza memoria: l'uscita dipende solamente dal valore dell'ingresso.
2. Sequenziali, l'uscita dipende dalla storia degli ingressi passati e non solo dal valore attuale in quanto hanno memoria, chiamata stato della rete.

2.2 Tabelle di verità

Rappresentano una maniera di speficcare una rete logica combinatoria, che elenca i valori delle uscite in corrispondenza delle combinazioni in ingresso.

2.3 Algebra di Boole

Rappresenta una maniera compatta di specificare le funzioni logiche tramite espressioni algebriche. Esistono tre operatori di base:

- AND: rappresentato come il simbolo del prodotto, produce 1 se entrambi gli operandi sono 1, 0 altrimenti.
- OR: rappresentato tramite il simbolo della somma, produce 1 se almeno uno degli operandi è 1, 0 altrimenti.

- NOT: rappresentato da una barra, inverte il valore logico.

Le leggi di de Morgan permettono di esprimere tutte le operazioni attraverso NAND o NOR.

2.4 Reti combinatorie

Non hanno notazione esplicita di tempo e non hanno memoria del passato.

2.4.1 Porte logiche

Sono dei circuiti elettronici che implementano gli operatori booleani fondamentali. Si possono combinare tra loro (in questo caso il not è un cerchio sull'input corrispondente).

Multiplexer

È un defiatore che sulla base di un input di controllo, determina quale degli input input gli passa. È composto da una serie di AND in parallelo che prendono in input quello effettivo e un controllo e sfociano in OR.

Programmable Logic Array

Per un multiplexer è una struttura che si compone di due stadi, una barriera di AND, la seconda una di OR. La sua dimensione totale è data dalla somma del piano AND e del piano Or. Ci sono porte logiche solo per le configurazioni di ingressi che producono 1 in uscita, se un mintermine è condifiso tra varie uscite lo si può riutilizzare (inserendolo una sola volta nel piano AND).

2.4.2 Costo

Le funzioni logiche possono essere implemetate in maniera più o meno efficiente, determinando il costo, ovvero la somma del numero di porte e del numero di ingressi della rete. È possibile trovare implementazioni della stessa rete con costi diversi.

2.4.3 Minimizzazione di funzioni logiche

È possibile ridurre delle espressioni logiche utilizzandone le regole algebriche, o metodi grafici non trattati.

2.4.4 Array di elementi logici

Molto spesso di costruiscono array di elementi che operano su dati complessi: per realizzare un multiplexer che opera su un bus a 32 bit utilizzando elementi a un bit. Si chiama BUS l'insieme dei fili che viene visto come un singolo segnale logico.

2.5 Reti sequenziali

Vengono introdotte per poter memorizzare informazioni attraverso una retroazione, ovvero si ridirezione l'uscita di alcune porte in ingresso ad altre porte del medesimo stadio in modo da formare un anello. La memoria viene generata un quanto gli ingressi ricordano il passato della rete attraverso il valore delle uscite passate (trasformate in nuovi input).

Elemento di base della memoria latch

Viene realizzato con due porte NOR nelle quali un input è preso dall'output dell'altra.

2.5.1 Stati indecidibili e temporizzazione

Dato che i segnali non si propagano in tempo nullo l'effetto del cambio di un ingresso si propaga in tempo finito sulle uscite che se fossero retroazionate potrebbe creare problemi di indecidibilità. Gli elementi di memoria sono pertanto temporizzati, governati da un segnale clock, un elemento di base di memoria temporizzato viene indicato come gated latch.

Gated latch

Il clock viene inserito come ingresso di abilitazione attraverso pore AND in quale uno dei due ingressi è il clock (che se a zero forza entrambi gli input a zero, pertanto la rete non può cambiare stato). Questi latch hanno stato indecidibile se entrambi gli input sono 1, si rimedia attraverso latch D nel quale gli ingressi al circuitop sono ottenuti da un'unica variabile che si nega, il circuito è abilitato durante tutta la fase positiva del clock. Flip-flop master-slave: presenta un master che passa un'uscita a uno slave che prende come input il negato del clock. L'uscita del circuito commuta al termine dell'impulsi di clock.

Capitolo 3

Assembly intel

Si basa su un'architettura CISC

3.1 Gestione dei registri

Per indicare un registro si prepone %, per un valore immediato $.Intel posside 16 registri a 64 bit general purpose: %rax, %rbx, %rcx, %rdx, %rsi, %rdi, %r8, %r9, %r10, %r11, %r12, %r13, %r14, %r15, %rbp il frame pointer e %rsp lo stack pointer. Per accedere ai 32 bit meno significativi si sostituisce r con e, per accedere ai 16 meno significativi si omette r, di questi 16 per accedere agli 8 più significatisi si prepone h, ai meno significativi l. Si trovano inoltre due registri specializzati: %rip instrucion pointer (program counter) e %rflags, ovvero il registro per i flags.

3.2 Convezioni di chiamata

Il passaggio di parametri di una funzione è considerato da 6 registri: %rsi, %rdi, %rcx, %rdx, %r8, %r9, mentre ulteriori argomenti possono essere salvati sullo stack. I valori di ritorno vengono salvati nei registri %rax e %rdx. I registri da preservare sono: %rbp, %rbx, %r12, %r13, %r14, %r15. Esistono due modalità per richiamare una funzione attraverso l'istruzione call: call address che chiama la subroutine all'indirizzo indicato e call *register che chiama la funzione all'indirizzo contenuto nel registro indicato. Il link register viene salvato automaticamente sullo stack, facilitando le funzioni ricorsive. L'istruzione ret preleva dallo stack l'indirizzo di ritorno da utilizzare nell'instrucion pointer.

3.3 Modalità di indirizzamento

Esistono varie modalità di indirizzamento in Intel:

- <displacement>

<displacement> (<base register>)

<displacement> (<index register>, [<scale>])

<displacement> (<index register>, <base register>, [<scale>])

L'indirizzo di memoria corrispondente viene calcolato come <displacement> + <base> + <index> · <scale>. Dove displacement è una costante a 8, 16, 32 o 64 bit, index e base sono indirizzi e scale è 1, 2, 4 o 8.

3.4 Sintassi istruzioni

Le istruzioni si presentano nella forma <opcode>[<size>]<source>, <destination>, dove il secondo elemento è sia operando che destinazione e deve essere un registro o un indirizzo di memoria. Il primo può essere un valore immediato. I due operandi non possono essere contemporaneamente indirizzi in memoria e non è possibile specificare due operandi e una destinazione diversa. <size> viene utilizzato per determinare la grandezza degli operandi: b per 8 bit, w per 16, l per 32, q per 64. È opzionale quando uno dei due operandi è un registro, obbligatorio altrimenti.

3.5 Istruzioni frequenti

A seguire un elenco delle istruzioni aritmetico-logiche più frequenti:

- mov per scambiare dati fra memoria e registri e viceversa (la destinazione non può essere un valore immediato);
- push e pop per leggere e salvare dati sullo stack, senza dover modificare lo stack pointer come avviene in MIPS;
- add (somma) e addc (somma con carry);
- sub (sottrazione) e subc (sottrazione con carry);
- mul (moltiplicazione con segno) e imul (moltiplicazione senza segno);
- div (divisione con segno) e idiv (divisione senza segno);
- inc (somma 1) e dec (sottrae 1);
- and, or, xor e not: operazioni logiche bit a bit;
- lea: load effective address;
- rcl, rcr, rol, ror: varie forme di rotate;
- sal, sar, shl, shr: shift aritmetico e logico;
- jmp: salto incondizionato;

- je (jump if equal), jnz (jump if not zero), jc (jump if carry), jnc (jump if not carry);
- neg;
- cmp: setta i flag facendo una sottrazione, ma senza salvarne il risultato;
- call e ret: indirizzo di ritorno sullo stack;
- nop;
- eventuali istruzioni condizionali.

Load effective address

Nonoestante questa operazione sia stata implementata per calcolare indirizzi con indirizzamento diverso senza effettuare accessi, risulta utile per effettuare la somma tra due registri e salvare il risultato in un terzo: lea (%rax, %rbx), %rcx. Nonostante la sintassi sia simile a quella di un indirizzamento non lo si sta effettuando.

Incremento e decremento

Utilizzate invece di add in quanto permettono di risparimiare 16 bit sull'operazione.

Capitolo 4

Assembly ARM

È un'architettura RISC pragmatica, tentando di migliorarla implementando istruzioni e strategie della Intel

4.1 Registri

In ARM sono presenti 16 registri a 32 bit, nominati da r0 a r15, non si utilizza un prrefisso per indicarli. r13 si riferisce allo stack pointer, r14 il link register (link all'indirizzo di ritorno delle subroutine), r15 il program counter.

4.2 Condizioni di chiamata

r0, r1, r2, r3, r12 sono registri temporanei, mentre da r4 a r11 sono da preservare, con l'eccezione di r9 per alcune ABI.

4.3 Istruzioni ARM

Sono simili al MIPS, ma meno regolari in quanto alcune possono presentare due argomenti. Nonostante sia RISC presenta una grande lista di istruzioni. Le istruzioni a tre argomenti prevedono il primo come destinazione e i successivi come operandi, se l'operando di sinistra deve essere un registro quello di destra può essere anche un valore immediato. I dati in memoria non possono essere utilizzati direttamente. Tutte le istruzioni permettono esecuzione condizionale grazie a suffissi al termine del nome identificativo dell'istruzione, la sua esecuzione avviene solo se i bit del registro di flag corrispondono alla condizione desiderata. I flag sono modificate da operazioni come cmp o da operazioni a cui si aggiunge il suffisso opzionale s che va a settare i bit del registro di flag. Lo schema di base di un'istruzione sarà: <opcode> [< −cond>][< −s>] <rd>,<rl >, <r*> dove [< −cond>][< −s>] sono facoltativi, rd è il registro di destinazione, r1 è il registro di destra e r* quello di sinistra o un valore immediato. L'operazione per

sommare due registri o un registro e un valore immediato rimane la stessa. Se il secondo operando è un registro al termine dell'operazione si possono inserire dei comandi ulteriori che permettono di eseguire operazioni di shifting o rotazione di esso.

4.3.1 Operazioni comuni

- add/adc: rispettivamente somma e somma con resto;
- sub/sbc: rispettivamente sottrazione e sottrazione con riporto;
- rsb/rsc: reverse sub/reverse sub with carry che permettono una sottrazione invertendo il primo ed il secondo operando. In questo modo risulta possibile sottrarre un registro ad un numero;
- and/orr/eor/bic: operazioni booleane bit a bit. Si noti che bic r0, r1, r calcola r0 = (r1 and (not r));
- mul/mla e simili sono per varie forme di moltiplicazione;
- b/bl rispettivamente branch e branch and link (da notare che è possibile aggiungere qualsiasi suffisso condizionale);
- bx è implementato solo in alcune CPU, corrisponde a move r15, r;
- cmp setta i flags comparando due operandi, ma senza risultato; da usarsi prima di salti condizionali. Funzionano similmente anche tst (attraverso un and) e teq (attraverso uno xor);
- ldr/str sono rispettivamente load register e store register. Rispecchiano rispettivamente lw e sw dell'assembly MIPS;
- mov/mvn: equivalente agli omonimi move e move not in MIPS; move notsposta il complemento a 1 del registro sorgente (utilizzata per implementare il not).

4.3.2 Operazioni sull'operando di destra

Le operazioni di shifting e rotating sul secondo operando prima dello svolgimento dell'operazione: add r0, r1, r2, lsl #2. Ovvero shifta a sinistra di 2 r2, poi esegue la somma.

4.3.3 Istruzioni di load store

Si possono salvare in memoria più registri con una sola istruzione ledm, stm con la seguente struttura ldm [−mode][−cond]rb[!], (lista dei registri). dove rb contiene la base, cond il suffisso condizionale come sopra e il suffisso mode può essere:

- ia: increment after, incrementa il registro base dopo l'esecuzione di ldm;

- ib: increment before, incrementa il registro base prima dell'esecuzione;
- da: decrement after, decrementa il registro base dopo l'esecuzione;
- db: decrement before, decrementa il registro base prima dell'esecuzione.

Il ! viene utilizzato per rendere definitive le modifiche approtate dai suffissi appena elencati dopo l'operazione.

4.4 Modalità di indirizzamento

Le modalità di indirizzamento che permettono di modificare il valore dell'indirizzo indicato dal secondo registro sono ldr e str. Esistono due modalità di indirizzamento ldr rd, rb (offset) e ldr rd, rb (index) [shift], dove rd è il registro destinazione, rb il registro dell'indirizzo di bse, offset un immediato a 12 bit e index è un valore in registro shiftato o ruotato. Si possono utilizzare meccanismi di pre indexing o post indexing:

- pre indexing con offset: [rb, #i]!, in questo caso la somma tra rb e i viene effettuata prima dell'indirizzamento, il ! è facoltativo e se è presente finalizza la somma (il valore di rb dopo l'esecuzione è dato da rb + i);
- post indexing con offset: [rb],#i!, in questo caso la somma tra rb e i viene effettuata dopo l'indirizzamento, il ! se è presente finalizza la somma (il valore di rb dopo l'esecuzione è dato da rb + i);
- pre indexing con indice e shift: [rb, ri, shift]!, in questo caso la somma tra rb e ri shiftato (si ricorda che lo shift è facoltativo) viene effettuata prima dell'indirizzamento, il ! se è presente finalizza la somma;
- post indexing con indice e shift: [rb], ri, shift !, in questo caso la somma tra rb e ri eventualmente shiftato viene effettuata dopo dell'indirizzamento.

Capitolo 5

Il processore

Si descriverà la struttura di un processore facendo riferimento a un set di istruzioni ridotto: accesso a memoria, aritmetico logiche e di salto. Le prime due fasi dell'esecuzione sono comuni a tutte le istruzioni e sono:

- Prelievo dell'istruzione da memoria.
- Lettura del valore di uno o più registri operandi estratti direttamente dai campi dell'istruzione.

Gli altri passi sono simili: tutte le istruzioni a parte quella di jump incondizionato utilizzano la ALU dopo aver letto gli operandi, o per calcolare l'indirizzo nel caso di istruzioni di accesso a memoria, il calcolo del risultato nel caso di operazioni logico-aritmetiche o per il calcolo del confronto nel caso delle operazioni di salto condizionato. Dopo l'utilizzo dell'ALU le operazioni si differenziano: le istruzioni di accesso a memoria richiedono o salvano il dato in memoria, le operazioni logico aritmetiche salvano il risultato nel registro target, le operazioni di salto condizionato cambiano il valore del program counter.

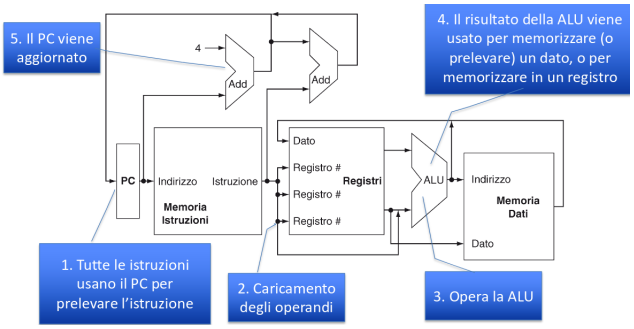

Figura 5.1: Un processore base

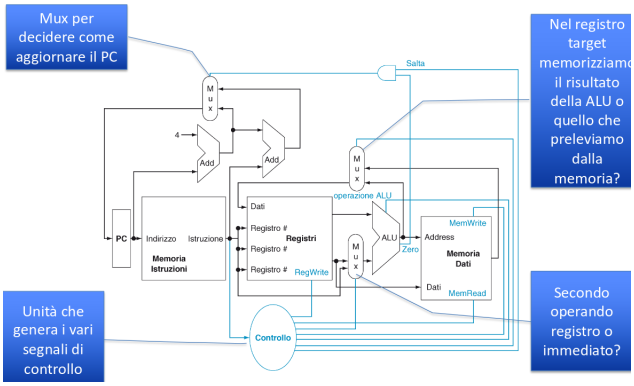

Figura 5.2: Un processore più dettagliato

La figura precedente è incompleta in quanto i dati arrivano da diverse sorgenti dalle quali bisogna scegliere, come per esempio per l'incremento del PC o la differenza tra istruzioni di tipo R o di tipo I, in cui un dato può provenire da un registro o essere contenuto nell'istruzione. Per selezionare quale delle operazioni svolgere viene utilizzato un multiplexer, che sulla base di un ingresso di controllo sceglie quale degli input debba finire in un output. Le linee di controllo del multiplexer vengono impostate sulla base del tipo di istruzioni. I vari gruppi funzionali hanno ulteriori ingressi di controllo: la ALU per decidere quale operazione effettuare, il banco registri ha un ingresso per decidere se scrivere in un ingresso o meno, la memoria dati ha degli ingressi per decidere se si vuole svolgere un'operazione di lettura o scrittura. La decisione dell'impiego degli ingressi di controllo è associata ad un'ulteriore unità funzionale.

Si può fare un'assunzione semplificativa dicendo che il processore lavora sincronizzandosi con i cicli di clock, e si assuma inoltre che tutte le operazioni si svolgano in un unico ciclo abbastanza lungo.

5.1 Temporizzazione

Questa metodologia esplicita quando i segnali possono essere letti o scritti in relazione al clock. Quella più utilizzata è quella sensibile ai fronti, in cui il dato viene memorizzato in corrispondenza della salita o della discesa del fronte di clock. I dati presi dagli elementi di stato sono relativi al ciclo precedente. Il tempo di clock deve essere scelto in modo da permettere ai dati di attraversare la rete combinatoria. Questa metodologia permette di rendere determinate operazioni che senza di essa sarebbero indecidibili.

5.2 realizzazione del datapath

Si passino in rassegna le componenti necessarie per realizzare un datapath:

- Una memoria istruzioni, dove sono salvate le istruzioni da eseguire.
- Il program counter, l'indirizzo dell'istruzione da eseguire.
- Il sommatore, un ALU specializzata a incrementare il PC.

Questi elementi permettono il prelievo dell'istruzione:

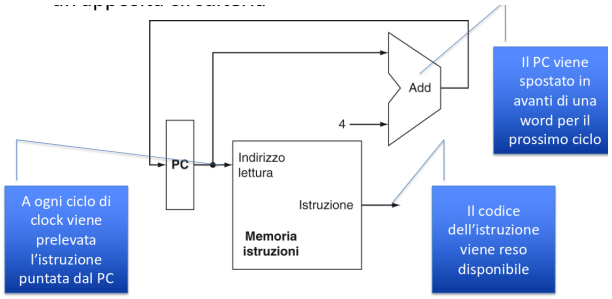

Figura 5.3: Il processo di prelievo di un'istruzione

5.2.1 Istruzioni di tipo R

Le operazioni di tipo R sono istruzioni aritmetico-logiche che operano tra registri e producono un risultato in un altro registro. Per operare queste operazioni si necessita di altri due blocchi funzionali:

- Il banco registri, che dà in output i registri specificati dell'istruzione e se abilitato in scrittura (regWrite) 0da un multiplexer scrive nel registro specificato il dato in ingresso.
- Una ALU che effettua l'operazione specificata da una codifica a 4 bit, setta un bit in uscita se il risultato è zero.

5.2.2 Istruzioni load store

Per entrambe si deve calcolare un indirizzo di memoria dato dalla somma di un registro con un offset e nel caso di un'operazione di scrittura leggere il registro dal register file. Si necessiterà ancora pertanto di ALU e register file. Si noti che essendo l'offset memorizzato in un campo a 16 bit occorrerà un'unità funzionale in grado di estendere il segno a 32 bit. Dovrà essere inoltre essere aggiunta un'unità di memoria dati da dove leggere e salvare i dati. Verrà utilizzata in scrittora (MemWrite) o in lettura (MemRead) in base al segnale dato dall'apposito multiplexer.

5.2.3 Salto condizionato

Per compiere un salto condizionato si necessita di sommare un offset che dovrà essere esteso a 32 bit al PC. Siccome quest ultimo verrà sempre automaticamente aumentato di 4 verrà aggiunto al PC già aumentato. L'offset inoltre viene automaticamente traslato di due bit in modo da esprimerlo come word e non come byte e estendento così l'intervallo degli offset raggiungibile. Occorre pertanto un ulteriore multiplexer che decida se operare sul PC un'operazione di Pc+4 o PC+4+offset. Per il salto incondizionato basta sostituire il campo offset shiftato di 4 al PC.

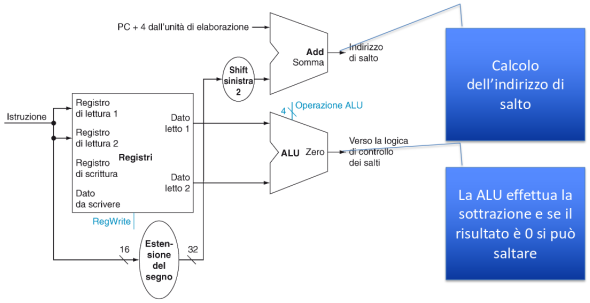

Figura 5.4: Il processo di Salto Condizionato

5.2.4 Progetto di un'unità di elaborazione

Siccome ogni unità funzionale può essere utilizzata un'unica volta per ogni ciclo di clock, si necessiterà di distinguere tra memoria dati e memoria istruzioni. Occorre inoltre condividere il più possibile le varie unità.

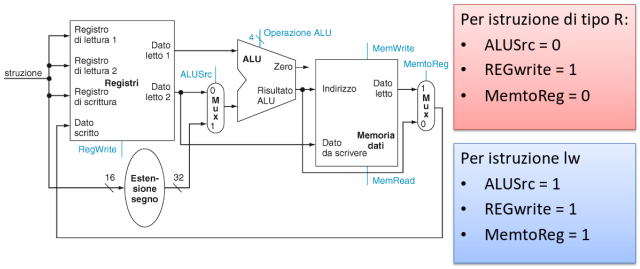

Figura 5.5: Circuito per istruzioni R e di trasferimento in memoria

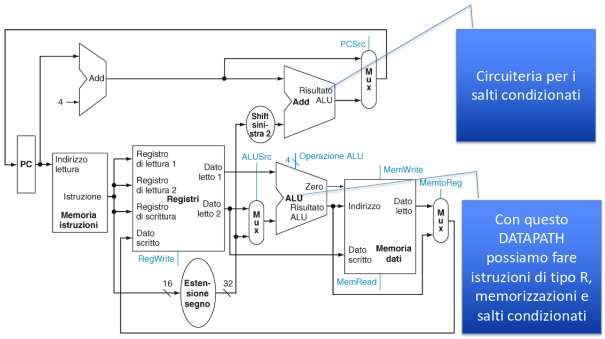

Figura 5.6: Circuito per istruzioni R e di trasferimento in memoria dettagliato

5.2.5 Prima implementazione comleta

Per arrivare a una prima implementazione completa si parta dal datapath mostrato e si aggiunga la parte di controllo, implementando le istruzioni add, sub, and, or, slt, lw, sw, beq e successivamente il jump.

ALU

La ALU viene utilizzata per realizzare operazioni logico aritmentiche di tipo R e slt, calcolare indirizzi di memoria e la sottrazione per beq. Per queste operazioni si ha una diversa configurazione degli input di controllo (a 4 bit), si veda la tabella sulle slide. Per generarli si utilizza un'unità di controllo che prende in ingresso il campo funct prelevato dall'istruzuione e due bit detti ALUop, ovvero 00 per sw e lw, 01 per beq, 10 per operazioni di tipo R specificate dal funct. Si genera pertanto un comando attraverso due livelli: il primo genera i segnali di controllo ALUop per l'unità di controllo della ALU, il secondo genera i segnali di controllo per la ALU. I segnali di controllo della ALU sono generati da una rete logica combinatoria e per evitare di elencare tutte le combinazioni di ingresso ALUop e dei campi funct vengono compressi attraverso l'utilizzo della wildcard X. Si vedano le tabelle delle slides.

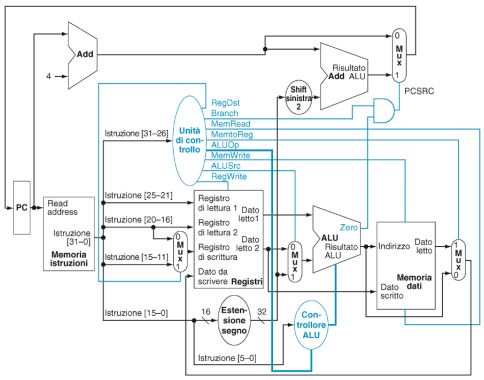

Figura 5.7: Una CPU molto dettagliata

Si faccia riferimento alle slides per una spiegazione dei segnali di controllo.

Unità di controllo

È un'unità funzionale combinatoria che prende come input il codice operativo dell'istruzione e genera i comandi del caso

Salto incondizionato

In questa operazione il PC viene incrementato di 4, i suoi quattro bit significativi rimangono uguali, dal 27 al 2 sostituiti con il campo indirizzo dell'istruzione i due bit meno significativi settati a 0.

5.3 Conclusione

Le istruzioni raramente vengono concluse in un unico ciclo in quanto sono le più lente a dettarlo e non si riesce a fare ottimizzazioni aggressive sulle cose più frequenti.

Capitolo 6

La pipeline

Si è notato come compiere un'operazione per ciclo di clock è inefficiente, pertanto si utilizza una pipeline. Si noti come le istruzioni del MIPS hanno 5 fasi di esecuzione: prelievo dell'istruzione dalla memoria, lettura dei registri e decodifica dell'istruzione, esecuzione di un'istruzione o calcolo di un indirizzo, accesso a un operando nella memoria dati, scrittura del risultato in un registro, verrà utilizzata pertanto una pipeline a 5 stadi. In una pipeline quando un istruzione termina l'utilizzo di un elmento funzionale questo viene subito occupato dall'istruzione successiva.

Confronto di prestazione

Il confronto può essere fatto come tempo fra due istruzioni=$\frac{Tempo\ tra\ due\ istruzioni\ senza\ pipeline}{numero\ stadi\ della\ pipeline}$.

6.1 Vantaggi del RISC

1. Essendo tutte le istruzioni della stessa lunghezza il prelievo è più facile.
2. Essendo i codici degli operandi in posizione fissa ci si può accedere leggendo il register file in parallelo con la decodifica dell'istruzione.
3. Gli operandi residienti in memoria sono utilizzabili solo da sw e lw, pertanto si può utilizzare la ALU per calcolare gli indirizzi. .
4. L'uso di accessi allineati permette agli accessi in memoria di avvenire in un solo ciclo impegnando un solo stadio della pipeline.

6.2 Hazard

In condizioni normali la pipeline permette di eseguire un'operazione per ciclo di clock, ma ci sono dei casi in cui questo non è possibile per il verificarsi di condizioni critiche.

6.2.1 Hazard strutturali

L'architettura del calcolatore rende impossibile l'esecuzione di alcune istruzioni in pipeline, ad esempio, disponendo di un'unica memoria non è possibile caricare istruzioni e prelevare operandi nello stesso ciclo di clok.

6.2.2 Hazard sui dati

Si verifica quando la pipeline deve essere messa in stallo per ottenere informazioni dagli stadi precedenti, come somme che utilizzando gli stessi operandi. Questo tipo di hazard blocca la pipeline per tre cicli di clock.

Possibili soluzioni

- In certi casi si può eliminare il problema a livello di compilatore invertendo delle istruzioni.
- È utile osservare come non è necessario salvare il risultato, attraverso un operazione di operand forwarding o propagazione, in cui il risultato viene reso disponibile bypassando l'operazione di storage.

6.2.3 Hazard sul controllo

Si verifica in presenza di salti condizionati, supponendo di avere un circuito sofisticato che permette di calcolare l'indirizzo di salto si necessita comunque di saltare uno o due cicli. Se la pipeline è troppo lunga questo stallo diventa troppo costoso. Vengono pertanto implementati dei circuiti che prevedano dei salti e fanno delle assunzioni su di essi, mettendo le operazioni nella pipeline in base ad esse e poi, se necessario si corregge. Si può considerare che il salto non venga utilizzato, o che il comportamento rimanga costante per esempio.

Capitolo 7

Le memorie

La memoria è fondamentale per il funzionamento di un compilatore. È necessario poterci leggere e scrivere dati. La memoria indirizzata direttamente (memoria principale o cache) è volatile ed è limitata dallo spazio di indirizzamento dal compilatore. Esiste una memoria indirizzata indirettamente o periferica, permanente con uno spazio di indirizzamento software non limitato dal processore. Le informazioni sulla memoria principale sono disponibili al processore in qualsiasi momento, mentre le informazioni nella memoria periferica devono essere prima trasferite a quella principale. Questo trasferimento è tipicamente mediato dal sistema operativo.

- Si intende per tempo di accesso il tempo di un'operazione di lettura o scrittura nella memoria.
- Il tempo di ciclo è il tempo che intercorre tra l'inizio di due operazioni tra locazioni diverse.
- Accesso casuale: non vi è alcuna relazione o ordine tra i dati salvati, tipico delle memorie a semiconduttori.
- Accesso sequenziale: l'accesso alla memoria è ordinato o semi ordinato, il tempo di accesso dipende dalla posizione, tipico dei dischi o dei nastri.
- RAM (random access memory) memoria scrivibile leggibile a semiconduttori, con tempo di accesso indipendente dalla posizione del dato.
- ROM (read only memory) memoria a semiconduttori in sola lettura può avere accesso casuale o sequenziale.

7.1 Memorie RAM a semiconduttori

Queste memorie memorizzano singoli bit spesso organizzati in byte e o word. Data una capacità N la memoria può essere organizzata in diversi modi a seconda

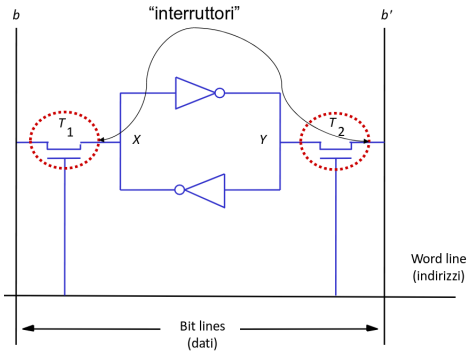

Figura 7.1: Un bit in SRAM

del parallelismo, influenzando il numero di pin I/O necessari al circuito integrato che la implementa.

7.1.1 Memorie statiche SRAM

Sono memorie in cui i bit possono essere salvati indefinitamente fintanto che rimangono alimentate, sono estremamente veloci e consumano poca corrente, ma sono care in quanto richiedono molte componenti per ciascuna cella di memorizzazione. Si consideri che $b = NOT(b')$, i circuiti di terminazione della linea di bit (sense/write circuit) interfacciano il mondo esterno che non accede mai direttamente alle celle, la loro presenza contemporanea riduce gli errori. In caso di scrittura la linea di word è alta e chiude T_1 e T_2, il valore presente su b e b', linee di pilotaggio viene salvato nel latch a doppio NOT. In caso di lettura la linea di word è alta e chiude T_1 e T_2, il le linee b e b' sono tenute in stato di alta impedenza e il valore in X e Y viene copiato in b e b'. Se la linea di word è bassa il consumo è nullo.

7.1.2 Memorie DRAM

Sono le memorie più diffuse in quanto economiche e a densità elevata, in quanto la memoria viene ottenuta sotto forma di carica di un condensatore. Hanno bisogno però di un costante refresh altrimenti la carica si disperderebbe a causa di correnti parassite. In caso di operazione di scrittura la linea di word è alta e chiude T e il valore di b viene copiato su C. In caso di lettura la linea di word chiude T e si utilizza un apposito circuito che se la tensione di C è sopra una certa soglia pilota la linea b alla tensione di alimentazione ricaricando C, altrimenti mette b a terra scaricando C.

Refresh

Nel momento in cui T è aperto il condensatore comincia a caricarsi o scaricarsi a causa di correnti parassite sul semiconduttore e si rende necessario quindi

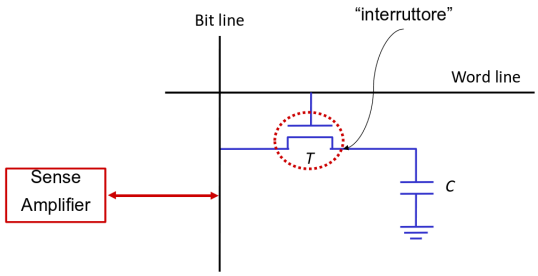

Figura 7.2: Un bit in DRAM

periodcamente rinfrescare i dati attraverso un'operazione di lettura. In genere la memoria contiene un circuito per la lettura periodica della memoria, pertanto l'utente non se ne deve preoccupare.

Multiplazione degli indirizzi

Data l'elevata integrazione delle DRAM il numero di pin I/O diventa un problema, pertanto è usuale multiplare nel tempo l'indirizzo delle righe e delle colonne negli stessi fili. Le memorie non sono indirizzabili al bit, per cui righe e colonne si riferiscono a byte e non a bit.

Modo di accesso veloce

L'accesso ai dati della memoria DRAM avviene da blocchi o pagine di memoria: l'indirizzo viene separato in row address selector e column address selector, il primo dei quali estrae una riga dalla pagina e il secondo la colonna dalla riga. È possibile, attraverso il fast page mode (FPM) evitare di riselezionare la riga ad ogni accesso se le posizioni sono consecutive con aumenti delle prestazioni significativi.

7.1.3 Memorie DRAM sincrone SDRAM

Le DRAM viste prima sono dette asincrone in quanto non esiste una precisa temporizzazione di accesso, ma la dinamica viene governata dai RAS e dai CAS. Il processore deve tenerne conto in quanto può generare problemi in fase di refresh. Aggiungendo dei buffer di memorizzazione degli ingressi e delle uscite si può ottenere un funzionamento sincrono disaccoppiando lettura e scrittura dal refresh, ottenendo automaticamente un FPM pilotato dal clock.

7.1.4 Double data rate SDRAM: DDR-SDRAM

Una SDRAM che consente il trasferimento dei file sia sul fronte positivo che quello negativo del clock. Latenza uguale a una DRAM normale ma banda

doppia, le memorie sono separate in due banchi uno per le locazioni pari sul fronte positivo e l'altro per le locazioni dispari sul fronte negativo. Le locazioni contigue sono in banchi separati pertanto si può fare un accesso interlacciato.

7.2 Velocità e prestazione

Latenza

Il tempo di accesso ad una singola parola, dà un indicazione al tempo che un processore dovrà aspettare un dato dalla memoria nel caso peggiore.

Velocità o banda

Indica la velocità di trasferimento massima in FPM, importante per operazioni in FPM che sono legate all'uso di memorie cache interne ai processori.

7.3 Gerarchie di memoria

Si può ottimizzare l'utilizzo di memorie in modo da dare l'impressione di avere una grande memoria veloce.

Località temporale

Quando si fa uso di una locazione è molto probabile che verrà riutilizzata presto.

Località spaziale

Quando si fa riferimento ad una locazione è molto probabile che nelle operazioni successive si farà riferimento alle locazioni successive.

7.3.1 Struttura della gerarchia

Costi e velocità delle memorie creano una propensione a utilizzare delle piccole e veloci vicino al processore che si ingrandiscono e rallentano allontanandosi da esso.

Terminologia

- Si indica con blocco l'unità minima di informazione che può essere presente o assente in un livello.
- Hit rate: la frequenza di accesso, la frazione degli accessi in cui trovo il blocco nel livello superiore.
- Miss rate: il complementare dell'hit rate.
- Tempo di hit: il tempo che occorre per trovare il dato quando lo trovo nel livello superiore.

- Penalità di miss: il tempo necessario per accedere al dato se non lo trovo nel livello superiore

La penalità di miss è molto maggiore del tempo di hit e del trasferimento in memoria di un singolo dato, pertanto è cruciale che non avvenga troppo spesso.

7.3.2 Cache

Un posto sicuro, o nascosto dove riporre i dati, nascosto in quanto è impossibile accedervi direttamente. Per capire se un dato è nella cache o no si può utilizzare una cache a mappatura diretta, ovvero a ogni indirizzo della memoria corrisponde una precisa locazione della cache, l'indirizzo di locazione dove un indirizzo è mappato è l'indirizzo del blocco modulo numero di blocchi nella cache. Se il numero di elementi della cache è a potenza di due è sufficiente prendere i bit meno significativi dell'indirizzo in numero pari al logaritmo in base due della potenza della cache. Siccome molte parole possono essere mappate sullo stesso blocco di cache per capire se in un dato momento vi si trova l'indirizzo ricercato si ricorre ad un campo, detto tag, che contiene informazione sufficiente a risalire al blocco correntemente salvato in memoria, si possono utilizzare per esempio i bit più significativi di una parola per trovare la locazione in cache dove l'indirizzo è mappato. Vengono utilizzati i bit più significativi per capire se nel blocco di cache viene memorizzato l'elemento richiesto, inoltre c'è un blocco di validità che dice se quello che viene memorizzato in un blocco di cache in un dato momento è quello richiesto.

Prestazioni

Blocchi di cache molto grande esaltano la località spaziale e diminuiscono la probabilità di miss. Tuttavia a parità di grandezza della cache blocchi molto grandi diminuisce l'efficacia della località temporale, oltre a generare dei miss con costo elevato. Si necessita pertanto di dover trovare un equilibrio.

Gestione delle miss

La presenza di una cache modifica la gestione della pipeline solo nel caso in cui ci sono delle miss, quando bisogna generare uno stallo nella pipeline per gestire il trasferimento da memoria principale a cache. Per una miss sulla memoria istruzioni bisognerà inviare alla memoria il valora PC-4, eseguire una lettura, scriverne il risultato aggiornando il tag e far ripartire la fetch. Gli accessi in lettura alla memoria dati avvengono alla stessa maniera.

Miss in scrittura

Gli accessi in scrittura sono delicati in quanto possono generare delle inconsistenze. Possono venire implementate due politiche:

1. Write-through, in cui ogni scrittura viene fatta direttamente in memoria principale, eliminando i problemi di consistenza ma aumentando i costi, si può impiegare un buffer di scrittura, una coda con tutte le scritture in attesa di essere completate.

2. Write-back, in cui se il blocco è in cache le scritture avvengono localmente in cache e l'update viene fatto solo quando il blocco viene rimpiazzato. Conveniente in presenza di numerose scritture.

Cache completamente associativa

In questo tipo di cache si può mappare qualsiasi tipo di blocco in qualsiasi blocco di cache, il loro problema è che rendono necesario cercare ovunque il dato, per essere efficiente su tutti i blocchi in parallelo, si necessitano pertanto n comparatori che operino su n blocchi. Il costo è molto elevato, pertanto viene utilizzata solo per cache molto piccole.

Cache set-associativa

È una via di mezzo tra la mappatura diretta e la completamente associativa: ogni blocco di memoria può essere mappato su una linea di n blocchi diversi di cache. Si combinano pertanto le due idee: a ciascun blocco di memoria viene associata una certa linea, pertanto uno degli n blocchi di quella liena su cui si può mappare il blocco di memoria e all'interno della linea si effettua una ricerca parallela come se fosse una cache completamente associativa. Ovvero un blocco di memoria viene mappato nella linea data da indirizzo blocco modulo numero linee della cache. Pertanto per trovare il blocco all'interno della linea si deve confrontare in parallelo il tag del blocco con tuti i tag dei blocchi di quella linea. Aumentando l'associatività diminuisce la frequenza di miss, ma si rendono necessarie operazioni complesse. Inoltre nelle cache a mappatura diretta in caso di miss so sicuramente chi sostituire, nelle cache associative si possono utilizzare diverse strategie, come una FIFO o una Least Recently Used.

Capitolo 8

Input-output

I dispositivi di I/O sono necessari al computer per comunicare con l'esterno, devono essere espandibili ed eterogenei. La tipologia di prestazione varia dai casi: nel caso di tastiere e mouse interessa più la latenza, nel caso di dischi o interfacce di rete interessa più il throughtput. Questi dispositivi sono collegati al processore da un dispositivo di comunicazione chiamato bus. I dispositivi i I/O possono essere classificati in base alle operazioni che compiono: read o write, in base al loro partner (uomo o macchina) e in base alla velocità di trasferimento.

8.1 Connesione tra processori e periferiche

Le connessioni avvengono tramite delle strutture di comunicazione chiamate bus che si possono dividere in due categorie:

1. Bus processore-memoria, specializzato, corto e veloce.
2. Bus I/O, possono essere lunghi e permettere la connessione con periferiche eterogenee, tipicamente non sono collegati direttamente alla memoria ma richiedono un bus processore-memoria o un bus di sistema.

Se prima era presente un unico bus parallelo che collegava tutto, ora per problemi di clock e frequenze troppo elevate si usano architetture composte da più bus paralleli condivisi e bus seriali punto-punto. Si indicherà con transizione I/O invio di indirizzo e spedizione o ricevimento di dati, con input il trasferimento di dati da una periferica verso una memoria dove il processore può leggerla, con output il trasferimento di dati dalla memoria al dispositivo.

8.1.1 Bus sincrono

Tra le linee di controllo di questo bus esiste un clock e le comunicazioni avvengono con un protocollo collegato al il ciclo di clock. Questo tipo di bus è molto semplice da implementare e molto veloce, ma presenta poca robustezza al drift del clock e necessita che tutte le periferiche vadano alla velocità del clock.

8.1.2 Bus asincrono

Per rimediare agli inconvenienti del bus sincrono si utilizza il bus asincrono, in cui tutte le transazioni sono governate da una serie di handshake e non più dal clock. Questo richiede l'introduzione di nuove linee di controllo per segnalare inizio e fine di transazioni ma permette di collegare periferiche con velocità diversa. Questo tipo di bus è robusto rispetto ai ritardi e consente di comunicare con periferiche di tipo diverso, ma è lento nelle connessioni in quanto richiede diversi segnali di controllo che devono circolare per permettere il passaggio di informazioni, la circuiteria di controllo è inoltre complessa. Si utilizzano spesso tecnologie ibride, ma prevalentemente asincrone. Il trend più recente è quello di implementare all'interno del processore gli hub per il controllo di I/O e della memoria.

8.2 Prospettiva del programmatore

Al programmatore interessa come trasformare una richiesta di I/O in un comando per la periferica e come trasferire i dati. Riguardo al sistema operativo occorre osservareche i programmi che condividono il processore condividono anche il sistema di I/O, i trasferimenti dati utilizzano delle interrupt che impattano le funzionalit à del SO, devono pertanto essere eseguiti in una modalità del processore detta supervisor cui solo il codice kernel può accedere, il controllo di I/O si interseca con problematiche di concorrenza. Un sistema operativo deve garantire che un utente con i permessi possa accedere ai sistemi di I/O cui può accedere, deve fornire comandi di alto livello per gestire operazioni di basso livello, gestire le interruzioni generate dall' I/O, ripartire l'accesso a un dispositivo tra i programmi che lo richiedono. Per implementare tali funzionalità occorre rendere possibile al SO di inviare comandi alle periferiche, rendere possibile ai dispositivi notificare il corretto avvenimento di un'operazione, consentire trasferimenti diretti tra dispositivi e memoria. Questo si fa fornendo sulle relative linee di bus delle parole di controllo scrivendo o leggendo in particolari locazioni di memoria (memory mapped I/O) o tramite delle istruzioni speciali legate all'I/O. Scrivendo una particolare parola in una locazione di memoria associata al dispositivo il sistema di memoria ignora la scrittura e il controllore di I/O intercetta l'indirizzo particolare e trasmette il dato al dispositivo sotto forma di comando. Queste particolari locazioni di memoria sono inaccessibili ai programmi utante ma solo al sistema operativo, pertanto deve esserci una chiamata di sistema che faccia commutare il processore in modalità supervisore. Il dispositivo può utilizzare queste locazioni per trasmettere dati o pre-segnalare il suo stato.

8.3 Trasmettere o ricevere dati

Per trasferire dati la maniera più semplice è l'attesa attiva o polling: si manda un comando di lettura scrittura alla periferica e si fa un ciclo di attesa testando

il bit di stato per vedere quando il dispositivo è pronto.

Costo del polling

Percentuale del processore utilizzata dal polling: prodotto tra frequenza di operazione e clock utilizzati dall'operazione di polling diviso la frequenza del processore.

8.3.1 Considerazioni

L'attesa attiva fa perdere tempo al processore che si dedica a cicli di lettura inutili, può pertanto essere utilizzato quando le operazioni avvengono con velocità determinata e se i dati vengono trasferiti con bitrate elevati il ciclo di attesa attiva dura poco. Se lo spreco è inaccettabile viene utilizzato I/O a interruzione di programma (interrupt driven I/O).

8.3.2 Interruzioni di programma

Un'interruzione I/O è un segnale utilizzato per segnalare al processore che la periferica è pronta a eseguire il trasferimento richiesto, possono avere diverso grado di urgenza e occorre un modo per segnalare al processore quale periferica richiede l'interruzione. Questo tipo di interruzioni sono sempre asincrone rispetto all'esecuzione delle istruzioni. Quando arriva un'interruzione l'istruzione corrente viene terminata prima di considerare l'interruzione. Si può differire l'esecuzione di un programma a un altro momento. Con questo metodo non occorre interrompere l'esecuzione del programma se non quando il dato può essere effettivamente riferito in memoria, ma si necessita di hardware speciale per interrompere l'esecuzione del programma per permettere alle periferiche di generare un'interruzione e per rilevare l'istruzione, salvare lo stato del processore per esegure una routine di servizio (Interrupt Service Routine ISR) e poi riprendere dal punto dove si era interrotto. Il guadagno rispetto al polling è che l'overhead necessario alla lettura dei dati viene pagato solo quando il dato è effettivamete presente.

8.4 Eccezioni

Un'eccezione è un trasferimento del controllo del programma non programmato. Il sistema effettua delle azioni per gestire le eccezioni, ome per esempio deve sapere dove registrare il punto di interruzione e dove salvare lo stato e poi, ad eccezione finita, come riprendere dal punto immediatamente successivo al punto di interruzione.

8.4.1 Interrupts

Sono eccezioni causate da eventi esterni, sono asincrone, possono essere gestite nello spazio tra due istruzioni, sospendono il programma e riprendono dallo stato in cui si era interrotto.

8.4.2 Traps

Sono eccezioni causate da eventi interni al programma, sincrone, gestite da un trap handler è possibile riprovare a eseguire l'istruzione che ha generato l'istruzione o abortire il programma.