

Notes Software Engineering

Brendon Mendicino

March 8, 2023

Contents

1	Memoria	3
1.1	Swapping	7
1.2	Esercizi	8
2	Memoria Virtuale	10
3	Rust	11

1 Memoria

La memoria si compone si suddivide in:

- registri;
- cache
- memoria primaria;
- memoria secondaria;

Uno principali problemi di accesso alla memoria è quello di assicurarne la sua protezione, ovvero evitare che un programma in memoria riesca ad accedere alle zone di memoria di altri programmi. Una volta fatto il bootstrap del SO, sia esso che i programmi verranno caricati in memoria, per evitare che ogni processo abbia una vista al di fuori del suo scope, si possono usare dei controlli a livello della CPU, esistono dei registri chiamati **base** e **limit**, che attraverso dei meccanismi, riescono ad effettuare la protezione della memoria. Esiste anche un altro problema che è quello **relocation**, consiste nel come mappare gli indirizzi delle varie istruzioni di salto e dei vari puntari una volta che il programma viene caricato in memoria, se si utilizzano degli indirizzi statici (creati solo in fase di compilazione e prendendo come riferimento di inizio del programma l'indirizzo 0), una volta che questo viene caricato in memoria le istruzioni non punterebbero più alle label corrispondenti ma sempre nello stesso punto, dove ad esempio si trova un altro programma. Per questo motivo quando si utilizzano valori di registri vengono sommati al base register, mentre le boundry del programma in memoria vengono salvate nel limit. Binding ... Si fa:

- **in compilazione:** fatto quando molto semplice, ad esempio quando esistono solo due programmi;
- **in fase di load:** viene fatta la rilocalizzazione durante il caricamento in memoria;
- **in esecuzione:** viene fatto il binding degli indirizzi in modo dinamico;

Per risolvere questo problema ci si affida all'hardware, che è incaricato di fare la traduzione: l'indirizzo rimane lo stesso (logico) all'interno del processore, prima di arrivare all'address bus viene tradotto in indirizzo fisico, esiste dunque una dicotomia di indirizzo logico e fisico, in questo modo quando si scrive un programma, l'indirizzo parte sempre da 0. Esistono due tipi di indirizzamento che sono di tipo logico, dove l'intervallo degli indirizzi utilizzabili è logico, ed un indirizzamento fisico, dove il range è limitato dalla memoria del sistema. Per effettuare questa traduzione da indirizzo fisico a indirizzo logico e viceversa si utilizza una **MMU** (Memory Management Unit). Il modo più facile per realizzare una MMU, è quello di usare un **relocation register**, ovvero un registro che contiene il valore da aggiungere un indirizzo logico per fare

un indirizzo fisico, il modello più semplice di MMU è fatto da un sommatore ed un comparatore.

Per aumentare le prestazioni ed usare la memoria in modo più efficiente si possono usare delle tecniche dinamiche.

- Si parla di **dynamic loading** quando, un programma viene caricato in memoria principale in modo frammentato, utilizzando solo i componenti che effettivamente vengono chiamati;
- Si parla di **dynamic linking** quando i file che contengono le funzioni che devono essere linkate (come le librerie standard) non vengono inserite all'interno dell'eseguibile, ma gli indirizzi vengono risolti in modo dinamico durante l'esecuzione;
- Il **link statico** è quando si crea un eseguibile con tutte le funzioni dentro, di fatto il loader carica tutto quando in memoria.

Il **dynamic loading** vuol dire che una routine non è caricata finché non è necessaria, questo può essere fatto quando il programmatore ne è consapevole, infatti il processo di load non è trasparente:

```
1 void myPrintf(**args) {  
2     static int loaded = 0;  
3     if (!loaded) {  
4         load("printf");  
5         loaded = 1;  
6     }  
7     printf(args);  
8 }
```

Il **linker-assisted DL** si usa una chiamata fasulla che prima chiama la load, usando una **stub**.

Le **shared libraries** sono in grado di condividere le risorse, infatti se più processi utilizzano la stessa funzione essa viene messa a disposizione e per ogni nuova chiamata non ci sarà bisogno di chiamare una load.

Come si alloca memoria per un programma (immagine)? La più semplice è l'allocazione contigua, dove si vede la RAM come due partizioni, una per il SO una per i processi (indirizzi più alti), per caricare un processo si parte da un indirizzo di inizio ed un indirizzo di fine, la MMU vista prima funziona solo con i casi di allocazione contigua (basilare). L'**allocazione contigua con partizione variabile**: quando ci sono più buchi ci sono delle politiche differenti per inserire nuovi programmi:

- **first-fit**: il primo che si trova;
- **best-fit**: il buco con la dimensione più piccola;
- **worst-fit**: il buco con la dimensione più grande;

La frammentazione è sparsità dei buchi all'interno della memoria. Si dice **esterna** perché è al di fuori dei processi, si dice **interna** quando è interna al processo, ovvero che ha più memoria di quello che serve. La frammentazione ha bisogno di **compattazione**, il SO sposta i pezzi e poi si riparte, partizione della memoria in zona libera e zona occupata, per fare una **deframmentazione** (o compattazione) vuol dire creare solo due partizioni (parte processi e zona libera), per effettuare la compattazione bisogna che i processi si possano spostare, inoltre un processo non può essere spostato se in quel momento il processo sta effettuando delle operazioni di IO, una soluzione per il problema dell'IO è il **latch job** in cui quella parte non può essere spostata, oppure si utilizza un **buffer IO del kernel**, si fa IO solo in buffer del sistema operativo.

Con **backing store** si definisce uno spazio della memoria secondaria in cui non si salvano programmi ma vengono immagazzinati dei dati che altrimenti dovrebbero andare in RAM.

La **Paginazione** risolve i problemi della allocazione continua, rimuovendo l'allocazione contigua al suo posto si utilizzano delle pagine, che sono l'unità minima di allocazione, questo risolve il problema della frammentazione.

Definition 1.1 – Pagine

Le partizioni della memoria logica.

Definition 1.2 – Frame

Le partizioni della memoria fisica.

Definition 1.3 – Blocco

...

Tipicamente la loro dimensione è un multiplo di due, sia pagine che frame hanno la stessa dimensione, da qualche parte andranno salvate le informazioni di mapping tra pagine e frame, si utilizza un **frame table**, dove ogni riga corrisponde a una mappatura. Anche utilizzando la paginazione si ha frammentazione interna, l'ultima pagina soffrirà di frammentazione.

Un indirizzo generato dalla CPU si divide in:

- **numero di pagine (p):**
- **numero di offset (d):**
- **numero di frame (f):**

Un indirizzo è composto da: (p-d, d)

Example 1.1

Se si hanno frame piccoli diminuisce la frammentazione ma aumentano anche le righe della tabella.

Nelle righe della tabelle si aggiungono dei bit in più:

- parte di protezione, specifica che la parte di codice non può essere scritta;
- **modify bit**: pagina modifica;
- **page present/absent**:

Come si implementa una page table? La page table si trova in memoria RAM, per sapere dove si trova si utilizzano due registri: **page table base register** e **base table lenght register**, infatti la base table si trova in memoria contigua. Per velocizzare questa operazione si utilizza che TLB che è più piccola e si trova direttamente sulla CPU, si usa la **Translation Look-aside Buffer** (TLB), un tipo di memoria in cui si accede per contenuto. Si aggiunge anche un'altra informazione **ASID** in cui viene salvata l'informazione del processo a cui la pagina appartiene, se non è presente questa informazione si i processi si contentano la TLB. Quando avviene un **TLB miss** se reinserisce nella TLB e poi si ritenta, utilizzando una politica scelta.

Lo schema finale è la combinazione di TLB e page table.

Il **Tempo di accesso effettivo** (EAT) in memoria è il tempo che mi costa accedere alla RAM:

$$EAT = h \cdot M + (1 - h) \cdot 2M$$

- h = TLB hit ratio;
- M = Memory access time;

La protezione è implementata associando un bit di protezione per un frame specifico, e quindi per la rispettiva pagina, grazie a questo bit si possono definire parti di codice che indica che il frame è in solo scrittura. Anche un altro bit associato è **validity** che indica quando una pagina è valida, ovvero quando c'è ed è associata ad un frame, o quando una pagina non è valida che vuol dire che la pagina non esiste o che non è associata ad frame, se si cerca di accedere una pagina non valida viene lanciata una **trap**.

La tabella della pagina permette di **condividere le pagine** (anche se in realtà sono i frame), se più processi hanno delle pagine che sono comuni vengono condivise da entrambi i processi.

La page table è una struttura dati del kernel:

Example 1.2

HP: spazio logico di indirizzamento di 32 bit, una pagina di 4KB (2^{12}), la page table avrà un milione di entry ($2^{32}/2^{12}$), ogni entry della page table sono 4bytes, quindi una pagetable è grande 4MB. Adesso è possibile avere:

- **page table contigua:**
 - dimensione critica (troppo grande):
 - * page table gerarchica;
 - * hash page table;
 - * inverted page table;

La **la page table gerarchica**, la page table viene divisa in blocchi più piccoli non contigui, se usa una page table di livello superiore che porte alle page table di livello inferiore, questi blocchi devono rimanere contigui, anche se diventano molto piccoli. Il page number viene diviso in due parti, una per la tabella outer ed una per la tabella inner (può avere anche più di due livelli), quando si va su 64 bit e la outer diventa molto grande si può usare solo una parte dell'indirizzamento se l'eseguibili è molto piccolo.

La **hashed page table** permette di creare una tabella di hash, con una funzione direttamente implementata in hardware che dato p in input ritorna f . Vanno implementate delle liste di collisione, e quindi viene immagazzinato che p che è la chiave di accesso. Usando una tabella di hash si potrebbe pensare anche di usare una page table condivisa tra tutti i processi, ma a quel punto va inserito anche l'ID del processo.

La **inverted page table** è una tabella condivisa tra tutti i processi, la sua grandezza viene dimensionata sulla grandezza della RAM e non sulla grandezza dei processi, in cui ogni frame fisico è associata una pagina, in questo caso le entry che corrisponde ad un frame ritorna la pagina a cui è associato, il problema che si vuole la traduzione da pagine ad entry e non il contrario, la prima strategia che si può utilizzare è la scansione lineare. Per rendere l'accesso più veloce viene messa una tabella di hash prima di arrivare alla tabella invertita.

1.1 Swapping

Si supponga che ad un certo punto si voglia far partire un processo e che la memoria sia piena, cosa si può fare? Una soluzione è lo **swapping**, ovvero viene rimesso sul backing store (in modo temporaneo) che in linux è la partizione di swap, e viene caricato il nuovo processo, grazie allo swapping si possono avere processi che hanno più memoria occupata di quanto la RAM sia grande.

Example 1.3

Quanto costa il **context switch**? Memoria piena e viene fatto partire un programma, dunque deve essere portato un processo nel backing store. 100MB da fare la swap con velocità di trasferimento di 50MB/sec.

- swap out = 2000ms
- più swap in dello stessa grandezza
- il tempo totale è di 4s

Se il processo sta facendo IO non si può fare lo swap out, una soluzione è non spostare un processo che sta facendo IO e spianare un altro, oppure usare un buffer del kernel.

Sui telefoni non esiste lo swapping, vengono in aiuto le **lifecycle dei contesti**. Il vantaggio di fare swapping è l'utilizzo del **paging swapping**, dove il swap in/out diventa page in/out, dove vengono trasferite solo le pagine e non l'intero processo.

1.2 Esercizi**Example 1.4**

- memoria fisica da 512MB
- allocazione minima 64B
- 128MB al SO
- tabella dei processi contiene: contiene indirizzo iniziale e size
- allocazione worst fit
- partizioni libere sono contenute in lista ordinata con dimensione decrescente
-

Si supponga ...

Example 1.5

Si descrivano brevemente

- tlb: 0.9 hit ratio
- page table a due livelli

- indirizzo in tre parti, 10 11 11 bit
-

Si fa una outer con cui si utilizzano 10bit, ed una inner con 11bit. Per calcolare il numero di inner ci sono due strade, il numero di byte preciso che contengono 100MB oppure si prende la prima potenza di 2 che contiene 100MB. Il resto delle righe delle outer overanno l'invalid bit settato ad 1.

2 Memoria Virtuale

Con **memoria virtuale** si indica che delle pagine esistono solo virtualmente ma non fisicamente, in questo modo si vuole supportare uno spazio di indirizzamento più grande dello spazio di indirizzamento fisico. Si parte dalla premessa che *un programma non bisogna di essere tutto in memoria per essere esguito*, si pensa ad un programma parzialmente caricato in memoria, dunque la memoria di un programma non è più vincolato dalla grandezza della RAM, in questo caso si parla di **memoria virtuale**. Avere questa memoria virtuale porta una serie di vantaggi che velocizzano tutte le operazioni di IO tra la RAM e la memoria secondaria. La conseguenza è che viene introdotta la **demand paging**, ovvero che una pagina viene caricata solo quando è richiesta. Il **demand paging** è molto simile allo swapping, infatti il caso limite è il **lazy swapper** dove inizialmente non si ha nessun frame caricato, e ogni richiesta viene preso un frame.

3 Rust

Rust è un linguaggio di programmazione moderno, che non permette di avere undefined behavior e soprattutto è **statically strongly typed**, inoltre è capace di inferire i tipi di dati. Rust inoltre fornisce delle *astrazioni a costo nullo*, rust è anche *interoperabile* con C. La memoria in rust è gestita dal programmatore solo in parte, il motivo è che il compilatore forza il programmatore a scrivere del codice senza errori. Esempio di **dangling pointer** in C.

```
1 typedef struct Dummy { int a; int b; } Dummy;
2
3 void foo(void) {
4     Dummy *ptr = (Dummy *)malloc(sizeof(Dummy));
5     Dummy *alias = ptr;
6     ptr->a = 2048;
7     free(ptr);
8     alias->b = 25;
9     free(alias);
10 }
```

Rust previene:

- dangling pointers
- doppi rilasci
- corse critiche
- buffer overflow
- iteratori invalidi
- overflow aritmetici

Inoltre rust propone delle convenzioni per aiutare il programmatore.

Rust parte dall'assunzione che un valore può essere **posseduta** da una singola variabile, se la variabile esce al di fuori del suo scope il valore viene deallocato. Quando si fanno delle assegnazioni l'**ownership** viene anche trasferito alla variabile assegnata, inoltre è anche possibile **dare in prestito (borrow)**, queste idee sono alla base della sicurezza di Rust. I puntatori sono tutti controllati in fase di compilazione, oltre all'**ownership** ogni puntatore ha un **tempo di vita (lifetime)**, tutti gli accessi al di fuori della lifetime sono negati dal compilatore, in alcuni non può essere fatto l'infering della lifetime e questo andrà specificato esplicitamente. La **sicurezza dei thread** è incorporata nel sistema dei tipi e anch'essi hanno una lifetime. Rust inoltre non ha stati nascosti, come in java con le eccezioni.

I due strumenti per gestire l'ambiente di sviluppo in rust sono:

- `$ rustup`: installer and updater di rust;

- `$ rustc`: compilatore;
- `$ cargo`: gestione dei progetti e delle dipendenze;

I comandi di base di `cargo` sono:

- `$ cargo new project-name`
- `$ cargo new --lib library-name`
- `$ cargo build`
- `$ cargo run`

Terminologia in rust:

- **crate**: unità di compilazione, crea un eseguibile o una libreria;
- **create root**: radice del progetto e solitamente contiene il `main.rs`, oppure `lib.rs` in caso di librerie;
- **module**: il progetto è organizzato in *moduli*, se si crea un modulo come cartella il file `.rs` andrà nominato `mod.rs`, all'interno possono essere presenti moduli interni;
- **package**:

Come in kotlin i blocchi condizionali hanno dei valori di ritorno. In rust non esiste l'ereditarietà, però esistono i **trait**, che sono simili alle interfacce, offrendo la possibilità di poter implementare dei metodi, ad esempio alcuni di questi sono `Display` e `Debug`, ogni tipo può implementare più tratti.

I tipi elementari di rust sono:

- numerici: `i8`, `i16`, `i32`, `i64`, `i128`, `isize` (valore nativo del processore).
- numerici senza segno: `u8`, ...
- naturali: `f32`, `f64`
- logici: `bool`
- caratteri: `char` (32 bit, rappresentazione **Unicode**)
- unit: `()` rappresenta una tupla di 0 elementi, corrisponde a `void` in C/C++

Per rappresentare le stringhe invece si use la codifica `utf-8`, che codifica i caratteri unicode in blocchi di 8 bit, la codifica utilizza la maggior parte dei primi 8 bit come caratteri standard, se si vogliono usare simboli più strani si combina un byte con il successivo, se il carattere è ancora più raro si utilizzano più byte, fino ad arrivare a 4.

Una tupla è una struttura che permette di contenere più tipi di valori, per accedere alla posizione corrispondente si utilizza la notazione `.<numero>`.

Rust ha un meccanismo al suo interno per rappresentare i puntatori, infatti quando viene creato un valore in una funzione si può decidere di passare la proprietà di questo alla funzione chiamante, che poi ha la responsabilità di liberarla oppure di passare ancora il possesso, in rust esistono tre tipi di puntatori:

- **reference;**
- **box;**
- **native pointer;**

Per utilizzare i puntatori nativi (che sono gli stessi del C), possono essere solo utilizzati in un blocco `unsafe ...`.

Le **reference** sono puntatori senza possesso e possono essere assegnati con `&`:

```
1 let r1 = &v;  
2 let r1 = &mut v;
```

In questo caso `r1` borrows il valore `v`, per acceder al valore si utilizza la notazione per **dereferenziare**: `*r1`. Quando si crea un puntatore che `&` si può un creare un puntatore in sola lettura, si vuole anche scrivere all'indirizzo del puntatore si deve usare la keyword `mut`: `&mut v`, l'accesso in scrittura è *esclusivo*, ovvero può essere assegnato ad una sola variabile e quando viene assegnato in modo mutabile nessun altro può utilizzarlo, infatti è *mutuamente esclusivo*.

```
1 fn main() {  
2     let mut i = 32;  
3  
4     let r = &i;      // r is of type "int ref";  
5     println!("{}", *r);  
6  
7     i = i+1;         // ERROR: i was borrowed  
8     println!("{}", *r);  
9 }
```

```
1 fn main() {  
2     let mut i = 32;  
3  
4     let r = &mut i;  
5     println!("{}", i); // ERROR: i was mutably borrowed  
6  
7     *r = *r+1;  
8     println!("{}", *r);  
9 }
```

In questo caso la variabile `i` non è accessibile in alcun modo per tutta l'esistenza di `r`.

In altre situazioni c'è l'esigenza di allocare un dato, per prolungare la sua vita all'infuori della funzione in cui viene creato, l'equivalente della `malloc` in rust è `Box<T>` che alloca una parte di memoria presa dall'*heap*, per creare un valore che si vuole venga conservato, si passa a `Box` il valore che voglio si venga conservato:

```
1 let b = Box::new(v);
```

Rust è in grado di fare l'infer del tipo di `v` e riesce ad allocare lo spazio necessario, quando `b` non sarà più visibile il `Box` verrà liberato dalla memoria.

```
1 fn useBox() {
2     let i = 4;                                // i si trova nello stack
3     let mut b = Box::new((5, 2));           // *b si trova nell'heap, b si
        trova nello stack
4
5     (*b).1 = 7;
6
7     println!("{:?}", *b);                   // (5, 7)
8     println!("{:?}", b);                   // (5, 7)
9 }
```

Quando `println!` si trova un puntatore lo dereferenzia automaticamente. Quando si arriva alla fine della funzione `a` e `b` vengono rimossi dallo stack, dato che il valore a cui puntava `b` non possiede un owner in vista quel valore viene rimosso dall'*heap*.

```
1 fn makeBox(a: i32) -> Box<(i32, i32)> {
2     let r = Box::new((a, 1));
3     return r;
4 }
5
6 fn main() {
7     let b = makeBox(5);
8     let c = b.0 + b.1;
9 }
```

In questo caso il valore l'ownership del valore puntato da `r` passa la sua ownership a `b` che si trova nel `main`, quando il `main` termina e la vita di `b` finisce il valore puntato viene anch'esso liberato.