Arquitectura de Microprocesadores

Carrera de Especialización en Sistemas Embebidos Universidad de Buenos Aires

**Preguntas orientadoras**

**Mansilla Rubén Darío Co20 CESE**

**1.** Describa brevemente los diferentes perfiles de familias de microprocesadores / microcontroladores de ARM. Explique alguna de sus diferencias características.

**Cortex M**

**1.** Describa brevemente las diferencias entre las familias de procesadores Cortex M0, M3 y M4.

**2.** ¿Por qué se dice que el set de instrucciones Thumb permite mayor densidad de código? Explique.

**3.** ¿Qué entiende por arquitectura load-store? ¿Qué tipo de instrucciones no posee este tipo de arquitectura?

**4.** ¿Cómo es el mapa de memoria de la familia?

**5.** ¿Qué ventajas presenta el uso de los “shadowed pointers” del PSP y el MSP?

**6.** Describa los diferentes modos de privilegio y operación del Cortex M, sus relaciones y como se conmuta de uno al otro. Describa un ejemplo en el que se pasa del modo privilegiado a no privilegiado y nuevamente a privilegiado.

**7.** ¿Qué se entiende por modelo de registros ortogonal? Dé un ejemplo

**8.** ¿Qué ventajas presenta el uso de instrucciones de ejecución condicional (IT)? Dé un ejemplo

**9.** Describa brevemente las excepciones más prioritarias (reset, NMI, Hardfault).

**10.** Describa las funciones principales de la pila. ¿Cómo resuelve la arquitectura el llamado a funciones y su retorno?

**11.** Describa la secuencia de reset del microprocesador.

**12.** ¿Qué entiende por “core peripherals”? ¿Qué diferencia existe entre estos y el resto de los periféricos?

**13.** ¿Cómo se implementan las prioridades de las interrupciones? Dé un ejemplo

**14.** ¿Qué es el CMSIS? ¿Qué función cumple? ¿Quién lo provee? ¿Qué ventajas aporta?

**15.** Cuando ocurre una interrupción, asumiendo que está habilitada ¿Cómo opera el microprocesador para atender a la subrutina correspondiente? Explique con un ejemplo

**16.** ¿Cómo cambia la operación de stacking al utilizar la unidad de punto flotante?

**17.** Explique las características avanzadas de atención a interrupciones: tail chaining y late arrival.

**18.** ¿Qué es el systick? ¿Por qué puede afirmarse que su implementación favorece la portabilidad de los sistemas operativos embebidos?

**19.** ¿Qué funciones cumple la unidad de protección de memoria (MPU)?

**20.** ¿Cuántas regiones pueden configurarse como máximo? ¿Qué ocurre en caso de haber solapamientos de las regiones? ¿Qué ocurre con las zonas de memoria no cubiertas por las regiones definidas?

**21.** ¿Para qué se suele utilizar la excepción PendSV? ¿Cómo se relaciona su uso con el resto de las excepciones? Dé un ejemplo

**22.** ¿Para qué se suele utilizar la excepción SVC? Explíquelo dentro de un marco de un sistema operativo embebido.

**ISA**

**1.** ¿Qué son los sufijos y para qué se los utiliza? Dé un ejemplo

**2.** ¿Para qué se utiliza el sufijo ‘s’? Dé un ejemplo

**3.** ¿Qué utilidad tiene la implementación de instrucciones de aritmética saturada? Dé un ejemplo con operaciones con datos de 8 bits.

**4.** Describa brevemente la interfaz entre assembler y C ¿Cómo se reciben los argumentos de las funciones? ¿Cómo se devuelve el resultado? ¿Qué registros deben guardarse en la pila antes de ser modificados?

**5.** ¿Qué es una instrucción SIMD? ¿En qué se aplican y que ventajas reporta su uso? Dé un ejemplo.

**Desarrollo**

**Preguntas orientadoras**

**1.** La familia de microprocesadores / microcontroladores de ARM está agrupada en tres tipos:

* **Cortex A (Application):** Esta familia está conformada por microprocesadores de Aplicación, de donde toma la sigla A. Constituida por microprocesadores de alto rendimiento orientados a soportar sistemas operativos embebidos de alta performance, y alto nivel de paralelismo.

Características principales:

* Contienen varios núcleos de alta frecuencia, del orden de los GHz.
* Tienen integrada mucha memoria RAM del orden de los GB.
* Tienen mucha memoria caché

Aplicaciones: Nintendo switch con las siguientes características:

* 4 Cortex A-57 trabajando a 1GHz
* 4 Cortex A-53 trabajando a 1,3 GHz
* 4 GB de memoria RAM LPDDR4
* **Cortex R (Realtime):** Esta familia está conformada por microprocesadores orientados a soportar sistemas de tiempo real donde se necesita implementar soluciones de baja. latencia, alta predictibilidad y elevada capacidad de cómputo. Por estas características se utilizan en sistemas críticos, como por ejemplo: sistemas de control para automóviles ( control de tracción, de frenos, ets), dispositivos médicos críticos, dispositivos industriales críticos, etc**.**
* **Cortex M (Microcontroller):** Son microcontroladores orientados a dispositivos de uso masivo y sistemas embebidos compactos. Están diseñados para soportar alta densidad de código y ser programados en C.

Los más conocidos son:

* **Cortex M0/M0+:** Pensados para una implementación mínima de bajo consumo y bajo costo.
* **Cortex M3/M4/M7:** Suman mayor performance, más funcionalidades (división por hardware), FPU (Unidad de Punto Flotante), MPU (Unidad de Protección de memoria), etc.

Ejemplos en placas de desarrollo: Imagen de la pantalla de un video juego

Descripción generada automáticamente con confianza media Un circuito electrónico

Descripción generada automáticamente con confianza media

PSOC 5LP: Cortex M3

Raspberry PI Pico: Cortex M0+

Imagen de la pantalla de un computador

Descripción generada automáticamente con confianza baja Imagen de la pantalla de un computador

Descripción generada automáticamente con confianza baja

STM32-Nucleo F676ZI: Cortex M7

STM32-Nucleo F429ZI: Cortex M4

**Cortex M**

**1.** Diferencias entre las familias de procesadores de ARM:

# Cortex M0 y M0+

* Tienen arquitectura ARMv6-M
* La mayoría soporta instrucciones Thumb (16 bits)
* Algunos soportan Thumb-2 (32 bits)
* Tienen multiplicación por hardware de 32 bits
* No tienen división por hardware
* No tienen solución “saturated math”
* No contienen extensión DSP (procesamiento de señales digitales)
* No incluyen FPU (Unidad de Punto Flotante)

# Cortex M3

* Tienen arquitectura ARMv7-M
* Todos soportan instrucciones Thumb (16 bits)
* Todos soportan Thumb-2 (32 bits)
* Tienen multiplicación por hardware de 32 bits o 64 bits
* Tienen división por hardware
* Tienen solución “saturated math”
* No contienen extensión DSP (procesamiento de señales digitales)
* No incluyen FPU (Unidad de Punto Flotante)

# Cortex M4

* Tienen arquitectura ARMv7E-M
* Todos soportan instrucciones Thumb (16 bits)
* Todos soportan Thumb-2 (32 bits)
* Tienen multiplicación por hardware de 32 bits o 64 bits
* Tienen división por hardware
* Tienen solución “saturated math”
* Contienen extensión DSP (procesamiento de señales digitales)
* Opcionalmente (SP) incluyen FPU (Unidad de Punto Flotante)

Cortex M7

* Tienen arquitectura ARMv7E-M
* Todos soportan instrucciones Thumb (16 bits)
* Todos soportan Thumb-2 (32 bits)
* Tienen multiplicación por hardware de 32 bits o 64 bits
* Tienen división por hardware
* Tienen solución “saturated math”
* Contienen extensión DSP (procesamiento de señales digitales)
* Opcionalmente (SP & DP) incluyen FPU (Unidad de Punto Flotante)

**2.** El set de instrucciones Thumb permite una mayor densidad de código en comparación con el set de instrucciones ARM tradicional, debido a que las instrucciones Thumb son instrucciones de 16 bits, mientras que las instrucciones ARM son de 32 bits. Esto puede ser beneficioso en términos de ahorro de memoria y aumento de la velocidad de transferencia de las instrucciones al microprocesador, aunque puede tener limitaciones en cuanto a la complejidad de las operaciones que se pueden realizar ya que necesitaría mas instrucciones thumb para resolver algunas tareas mas complejas.

**3.** La arquitectura load-store es un tipo de arquitectura en la que solo se pueden realizar operaciones de carga (load) y almacenamiento (store) entre la memoria y los registros, mientras que las operaciones aritméticas se realizan exclusivamente entre registros.

En una arquitectura load-store, las instrucciones de carga (load) se utilizan para transferir datos desde la memoria a los registros, mientras que las instrucciones de almacenamiento (store) se utilizan para transferir datos desde los registros a la memoria.

Este tipo de arquitectura **no permite realizar operaciones aritméticas** directamente entre la memoria y los registros. Por lo tanto, l**as instrucciones que implican operaciones aritméticas con operandos en la memoria**, como por ejemplo "add" (suma) o "sub" (resta), n**o están disponibles** en una arquitectura load-store.

En resumen, una arquitectura load-store es aquella en la que las operaciones de carga y almacenamiento se realizan entre la memoria y los registros, mientras que las operaciones aritméticas se realizan exclusivamente entre registros.

**4.** El mapa de memoria de la familia ARM varía dependiendo del modelo específico y la implementación de la arquitectura. Sin embargo, en términos generales, la familia ARM utiliza una estructura de memoria en la que se divide el espacio de direcciones en diferentes regiones.

A modo de descripción general del mapa de memoria típico de la familia ARM, podemos considerar la siguiente subdivisión de regiones:

* Zona de código (Code Section): Esta zona se utiliza para almacenar el código ejecutable, como las instrucciones del programa y las constantes. Es una región de solo lectura (read-only) y suele estar ubicada en la parte inferior del espacio de direcciones.
* Zona de datos (Data Section): Esta zona se utiliza para almacenar los datos del programa, como variables globales y estáticas. Puede ser de lectura y escritura (read-write) y suele estar ubicada en la parte superior del espacio de direcciones.
* Pila (Stack): La pila se utiliza para almacenar las variables locales y los registros de activación de las funciones. Generalmente crece hacia abajo en la memoria y se encuentra en la parte superior del espacio de direcciones.
* Montón (Heap): El montón se utiliza para almacenar datos dinámicos, como objetos o estructuras de datos creados en tiempo de ejecución. Generalmente crece hacia arriba en la memoria y se encuentra en la parte inferior del espacio de direcciones.
* Además de estas regiones principales, también puede haber otras regiones en el mapa de memoria, como zonas reservadas para el sistema operativo, controladores de dispositivos, tablas de vectores de interrupción, entre otros.

|------------------------------------|

| Zona de código (ROM) |

|------------------------------------|

| Zona de código (RAM) |

|------------------------------------|

| Zona de datos (RAM) |

|------------------------------------|

| Pila |

|------------------------------------|

| Montón |

|------------------------------------|

| Zona de dispositivos |

|------------------------------------|

| Zona de sistema |

|------------------------------------|

**5.** El uso de "shadowed pointers" (punteros en sombra) en el PSP (Process Stack Pointer) y el MSP (Main Stack Pointer) en la arquitectura ARM presenta varias ventajas:

* Seguridad: Los "shadowed pointers" permiten tener una copia de seguridad de los punteros de pila principales (PSP y MSP). Esto es útil en caso de que se produzca un desbordamiento de pila o un error en el programa, ya que se puede acceder a la copia en sombra para recuperar la integridad del sistema.
* Protección contra overflow (desbordamiento) de pila: El uso de "shadowed pointers" puede ayudar a detectar y proteger contra desbordamientos de pila. Si se produce un overflow en el PSP o el MSP, la copia en sombra se mantendrá intacta y se podrá utilizar para detectar el overflow y tomar medidas correctivas.
* Facilidad de depuración: Al tener una copia en sombra de los punteros de pila, se facilita la depuración de errores relacionados con la pila. Se pueden utilizar herramientas de depuración para comparar los valores de los punteros en sombra con los valores actuales y detectar cualquier discrepancia o anomalía.
* Recuperación de errores: En caso de que se produzca un error crítico en el programa y se pierda la integridad de los punteros de pila principales, los "shadowed pointers" pueden utilizarse para recuperar el sistema y restaurar los valores correctos de los punteros de pila.

En resumen, el uso de "shadowed pointers" en el PSP y el MSP proporciona una capa adicional de seguridad y protección contra desbordamientos de pila, facilita la depuración de errores relacionados con la pila y permite la recuperación del sistema en caso de errores críticos.

**6.** El procesador Cortex-M de ARM utiliza un modelo de seguridad basado en modos de privilegio y operación para garantizar la protección y el aislamiento entre diferentes niveles de software. Los modos de privilegio y operación en el Cortex-M son los siguientes:

* Modo Handler (Privilegiado): Este modo es el más alto en términos de privilegios y se utiliza para ejecutar rutinas de manejo de excepciones y eventos, como interrupciones y excepciones de sistema. En este modo, se tiene acceso completo a todas las instrucciones y registros del procesador.
* Modo Thread (Privilegiado): Este modo se utiliza para la ejecución de tareas normales del programa. En este modo, se tiene acceso completo a todas las instrucciones y registros del procesador.
* Modo Unprivileged (No privilegiado): Este modo es el de menor privilegio y se utiliza para ejecutar tareas con restricciones de seguridad. En este modo, se restringe el acceso a ciertas instrucciones y registros del procesador, lo que ayuda a proteger el sistema operativo y las aplicaciones de software de posibles amenazas.

La conmutación entre los diferentes modos de privilegio y operación se realiza mediante el cambio de bits específicos en el registro de estado (PSR) del procesador. El bit de Control (CONTROL) en el PSR se utiliza para habilitar o deshabilitar el cambio de modo privilegiado a no privilegiado y viceversa.

A continuación, se describe un ejemplo de cómo se pasa del modo privilegiado al no privilegiado y nuevamente al modo privilegiado:

* Inicialmente, el procesador se encuentra en el modo privilegiado (Modo Handler o Modo Thread).
* Se ejecuta una instrucción que cambia el bit de Control en el PSR para habilitar el modo no privilegiado.
* A partir de ese momento, el procesador se encuentra en el modo no privilegiado, donde se restringe el acceso a ciertas instrucciones y registros.
* Durante la ejecución en el modo no privilegiado, se produce una excepción o interrupción.
* El procesador cambia automáticamente al modo privilegiado (Modo Handler) para manejar la excepción o interrupción.
* Una vez finalizada la rutina de manejo de excepciones, se ejecuta una instrucción que cambia nuevamente el bit de Control en el PSR para habilitar el modo privilegiado.
* A partir de ese momento, el procesador se encuentra nuevamente en el modo privilegiado (Modo Handler o Modo Thread).

No se puede regresar directamente del modo no privilegiado al modo privilegiado. Si se desea hacerlo, se debe disparar una interrupción o excepción que saque al sistema del modo no privilegiado y lo lleve al modo Handler (privilegiado); sólo estando en un modo privilegiado se puede cambiar el bit de control de PSR para habilitar el modo privilegiado.

**7.** Se dice que la arquitectura ARM cuenta con un modelo de registros ortogonal porque la configuración de cada registro no interfiere en la del otro. El contenido de cada registro no afecta al contenido del otro.

Por ejemplo, cuando se utiliza un sistema operativo embebido, el registro CONTROL podría re programarse en cada cambio de contexto para permitir que algunas tareas de la aplicación se ejecuten con un nivel de acceso privilegiado y otras se ejecuten con un nivel de acceso sin privilegios.

Decimos que las configuraciones de nPRIV y SPSEL son ortogonales, dado que son posibles cuatro combinaciones diferentes de nPRIV y SPSEL, aunque sólo tres de ellas se usan comúnmente en aplicaciones del mundo real.

En la mayoría de las aplicaciones simples sin un sistema operativo embebido, no es necesario cambiar el valor del registro CONTROL. Toda la aplicación puede ejecutarse en un nivel de acceso privilegiado y utilizar únicamente el MSP.

**8.** Las instrucciones de ejecución condicional (IT, por sus siglas en inglés) son una característica de la arquitectura ARM que permite ejecutar instrucciones condicionalmente en función del estado de las banderas o flags del procesador. Estas instrucciones ofrecen varias ventajas, entre las que se incluyen:

* Reducción del tamaño del código: Las instrucciones condicionales permiten ejecutar diferentes instrucciones en función de una condición, lo que puede eliminar la necesidad de escribir múltiples bloques de código separados. Esto reduce el tamaño del código y facilita su mantenimiento.
* Mejora del rendimiento: Al ejecutar instrucciones condicionalmente, se pueden evitar saltos o desvíos innecesarios, lo que puede mejorar el rendimiento del programa al reducir la cantidad de ciclos de reloj necesarios para ejecutarlo.
* Mayor flexibilidad: Las instrucciones condicionales permiten adaptar el flujo de ejecución del programa según diferentes condiciones, lo que brinda una mayor flexibilidad en el diseño del software. Esto puede ser especialmente útil en casos donde se necesitan tomar decisiones basadas en múltiples condiciones.
* Optimización del código: Al utilizar instrucciones condicionales, el compilador puede realizar diferentes optimizaciones, como la eliminación de código muerto o la reorganización de instrucciones para aprovechar al máximo el pipeline del procesador.

Un ejemplo de uso de instrucciones de ejecución condicional en ARM sería:

```

CMP R0, #0 ; Compara el valor de R0 con 0

ITE GT ; Ejecuta las siguientes dos instrucciones si R0 es mayor que 0

MOVGT R1, #1 ; Si R0 > 0, mueve el valor 1 a R1

MOVLE R1, #0 ; Si R0 <= 0, mueve el valor 0 a R1

```

En este ejemplo, se compara el valor de R0 con 0 y, dependiendo del resultado de la comparación, se ejecutan diferentes instrucciones. Si R0 es mayor que 0, se mueve el valor 1 a R1. Si R0 es menor o igual a 0, se mueve el valor 0 a R1. Esto permite tomar diferentes acciones en función de una condición específica.