



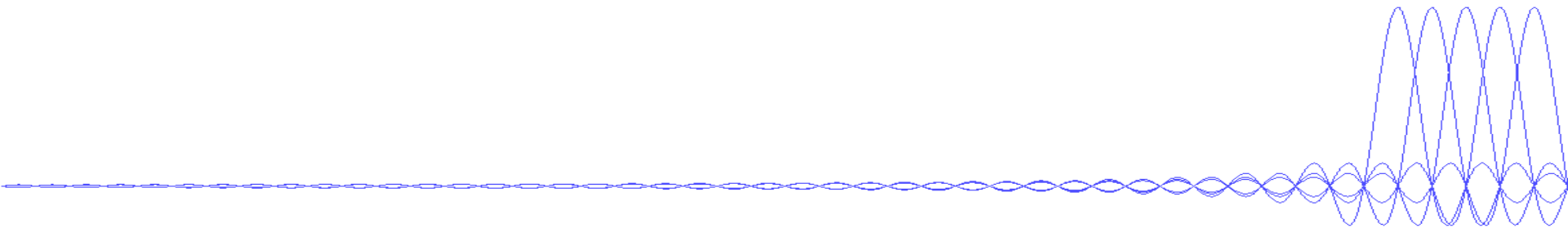
COMPUTER ENGINEERING



**UIT**  
TRƯỜNG ĐẠI HỌC  
CÔNG NGHỆ THÔNG TIN

# TỔ CHỨC VÀ CẤU TRÚC MÁY TÍNH II

## Chương 7 Biên dịch chương trình

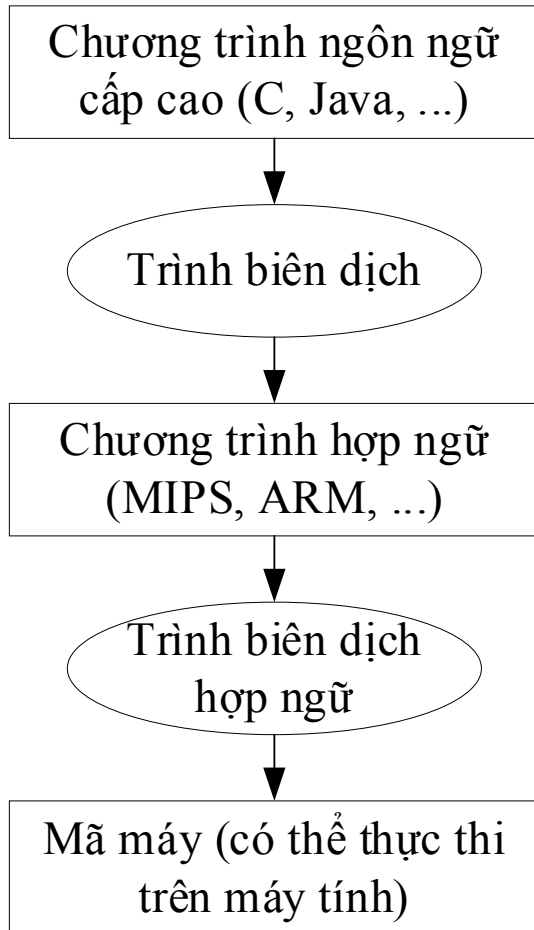




- Trình biên dịch (Compiler)
- Trình biên dịch hợp ngữ (Assembler)
- Biên dịch ngược (Reverse-Engineering)
- Bài tập



# Trình biên dịch (1/2)

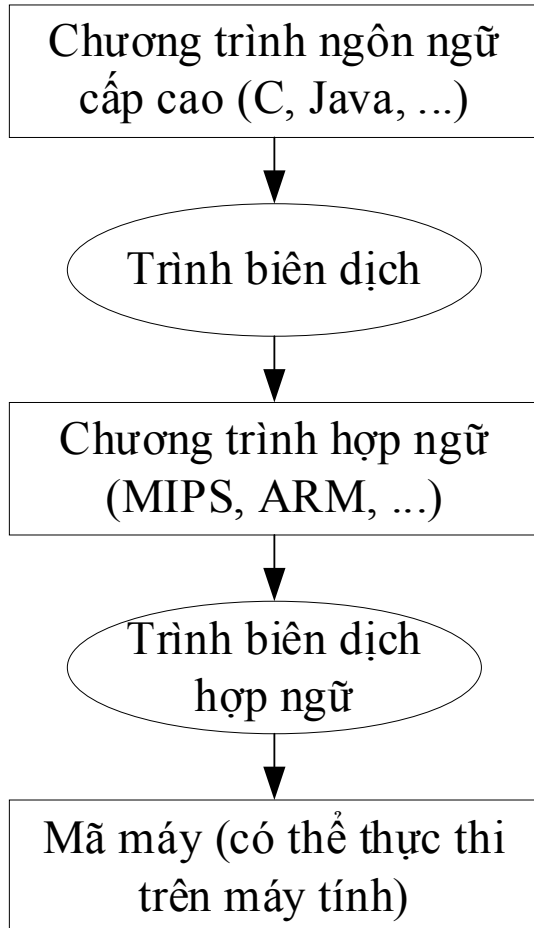


■ Trình biên dịch có chức năng chuyển chương trình được viết bởi ngôn ngữ lập trình cấp cao thành chương trình hợp ngữ:

- Ngôn ngữ lập trình cấp cao (C, Java, ...) gần với suy nghĩ con người và độc lập phần cứng
- Hợp ngữ (MIPS, ARM, ...) là một ngôn ngữ gọi nhớ của mã máy, phụ thuộc phần cứng



# Trình biên dịch (2/2) – Ví dụ



```
if(a == b)
    c = 2;
else
    c = -1;
d = a + c;
```

```
bne $a0, $a1, ELSE
addi $s0, $0, 2
j     ENDIF
ELSE:
    addi $s0, $0, -1
ENDIF:
    add $s1, $a0, $s0
```



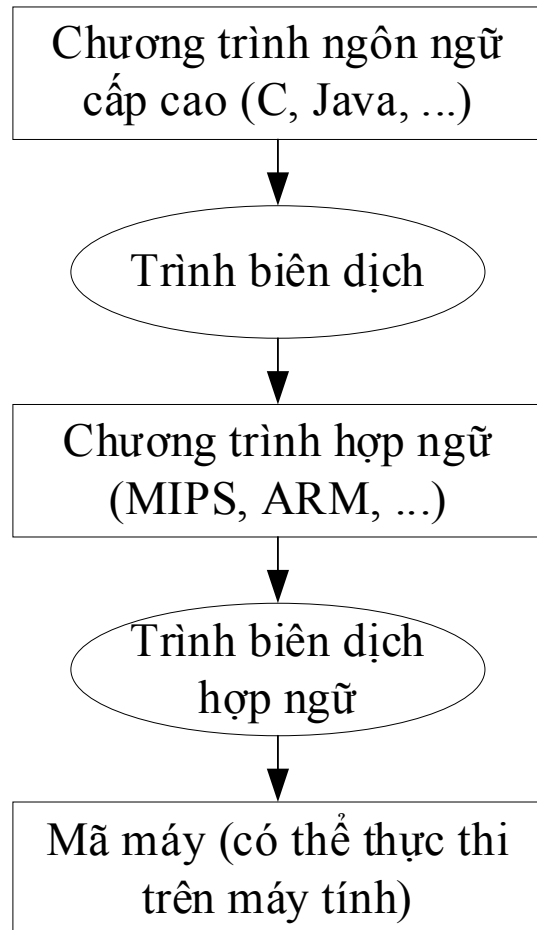
# Quiz 1

- Biên dịch chương trình được viết bằng ngôn ngữ C sau sang hợp ngữ MIPS

```
int arraylength = 5;  
for(int i = 0; i < arraylength; i++){  
    arrayvalue[i] = i;  
}
```



# Trình biên dịch hợp ngữ (1/2)



- Trình biên dịch hợp ngữ có chức năng chuyển chương trình được viết bởi hợp ngữ thành mã máy:

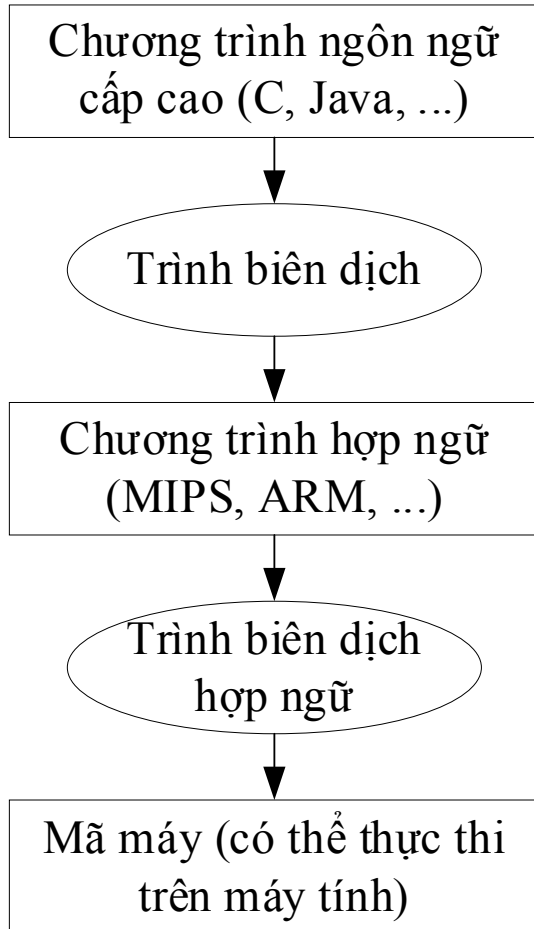
- Mã máy là các chuỗi bit (0, 1) có thể được thực thi trên máy tính

- Có thể sử dụng lệnh giả (pseudo instruction) để viết chương trình hợp ngữ nhằm đơn giản hơn cho lập trình viên

- Lệnh giả: Không phải lệnh thực sự của máy nhưng trình biên dịch có thể chuyển thành lệnh thực sự



# Trình biên dịch hợp ngữ (2/2)



la	\$a0, exit	0x3c010040
li	\$a1, 50	0x3424001c
add	\$t1, \$t2, \$t1	0x24050032
addi	\$t1, \$a0, 0	0x01494820
bne	\$a1, \$t1, exit	0x20890000
lw	\$a3, 4(\$t1)	0x14a90001
exit:		0x8d270004
		...



## Quiz 2

- Biên dịch chương trình được viết bằng hợp ngữ MIPS bên cạnh sang mã máy, biết rằng chương trình bắt đầu ở địa chỉ 0x000C0

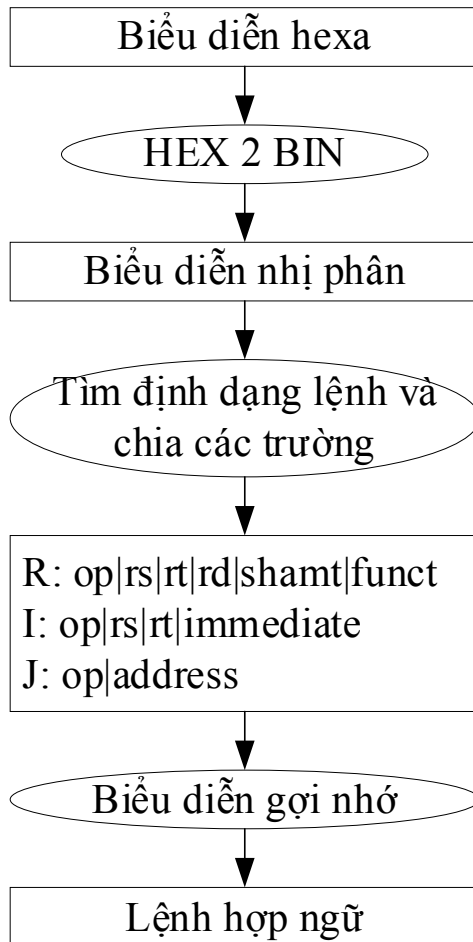
```
bne $s0, $s1, FAIL
add $s2, $0, $0
j    END
FAIL: addi $s2, $0, -1
END:
```





# Biên dịch ngược

COMPUTER ENGINEERING



■ Biên dịch ngược là quá trình khôi phục mã máy thành chương trình hợp ngữ

0x00af8020

0000 0000 1010 1111 1000 0000 0010 0000

000000 00101 01111 10000 00000 100000

add \$16, \$5, \$15 hoặc add \$s0, \$a1, \$t7



# Bài tập

- Biên dịch chương trình chương trình được viết bằng ngôn ngữ lập trình C sang hợp ngữ MIPS, sau đó biên dịch sang mã máy

```
int count = 1;  
while(count <= 20){  
    arrayA[count - 1] = arrayB[count + 2];  
    count++;  
}
```



COMPUTER ENGINEERING

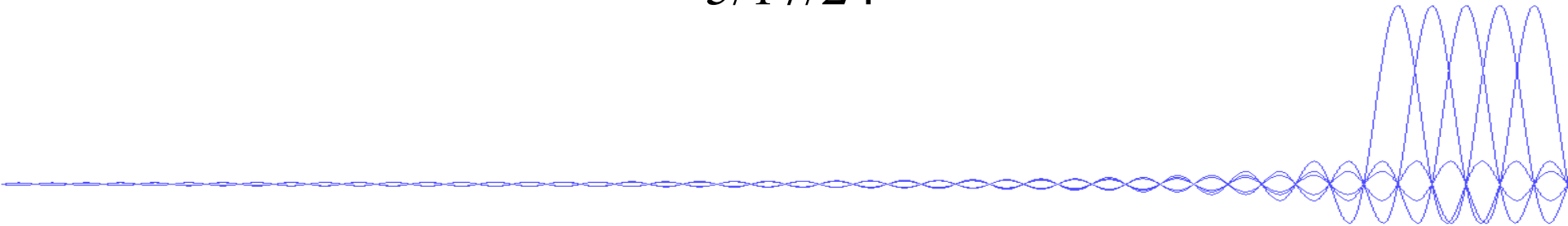


**UIT**  
TRƯỜNG ĐẠI HỌC  
CÔNG NGHỆ THÔNG TIN

# TỔ CHỨC VÀ CẤU TRÚC MÁY TÍNH II

## Ôn tập Kiến trúc tập lệnh

5/17/24





- Thực thi chương trình
- Chuyển từ C sang MIPS
- Chuyển từ MIPS sang C
- Chuyển từ MIPS sang mã máy
- Chuyển từ mã máy sang MIPS
- Bài tập



# Thực thi chương trình (1/2)

- Giá trị của thanh ghi \$v0 và \$v1 là bao nhiêu sau khi thực thi chương trình bên dưới

```
lui    $t0, 0x5678
addi   $t1, $0, 0x4321
or     $a0, $t0, $t1
nor    $a1, $a0, $0
slt    $v0, $t0, $a0
sltu   $v1, $t1, $a1
```



## Thực thi chương trình (2/2)

- Giá trị của thanh ghi \$v0 và \$v1 là bao nhiêu sau khi thực thi chương trình bên dưới

```
addi $a0, $0, 0x1234
```

```
addi $a1, $0, 0xCAFE
```

```
addi $t1, $0, 0x432C
```

```
sw    $a0, 0($t1)
```

```
addi $t1, $t1, 4
```

```
sw    $a1, 4($t1)
```

```
lw    $v0, -8($t1)
```

```
lw    $v1, 0($t1)
```



# Chuyển từ C sang MIPS (1/2)

Cho chương trình C bên dưới. Biết rằng  $g$ ,  $h$ ,  $i$ ,  $j$  là những biến nguyên 32 bit, trả lời các câu hỏi sau:

- ☐ Tìm mã hợp ngữ MIPS tương đương của chương trình.
- ☐ Cần bao nhiêu lệnh MIPS để hiện thực chương trình
- ☐ Nếu các biến  $g$ ,  $h$ ,  $i$  và  $j$  có giá trị tương ứng là 1, 2, 3, 4, 5 thì giá trị của  $f$  và  $k$  là bao nhiêu?

$$f = g + h + i + j$$
$$k = g + (h + 5)$$



# Chuyển từ C sang MIPS (2/2)

Cho câu lệnh C:  $f = g - A[B[4]]$ ;

- Tìm mã MIPS tương đương của chương trình nếu địa chỉ của mảng A và B lần lượt nằm trong các thanh ghi \$s6 và \$s7. Biến g là biến nguyên 32 bit.





# Chuyển từ MIPS sang C (1/2)

- Tìm chương trình C tương ứng với chương trình hợp ngữ MIPS bên dưới

```
add $t0, $a0, $a1
```

```
addi $t1, $a0, 5
```

```
sub $t2, $t0, $a1
```

```
add $s0, $t2, $a2
```



# Chuyển từ MIPS sang C (2/2)

- Tìm chương trình C tương ứng với chương trình hợp ngữ MIPS bên dưới

```
bne $a0, $a1, another
```

```
add $s0, $0, $0
```

```
j exit
```

```
another: addi $s0, $s0, -1
```

```
exit:
```



# Chuyển từ MIPS sang mã máy

- Chuyển chương trình hợp ngữ MIPS bên dưới sang mã máy

```
        add $t0, $t0, $zero
Loop:   lw  $t1, 4($s3)
        addi $s3, $s3, 4
        bne $t1, $t0, Loop
```



# Chuyển từ mã máy sang MIPS

- Chuyển chương trình được lưu trong bộ nhớ bên dưới sang hợp ngữ MIPS

0x00a6202a

0x2149ff90



# THẢO LUẬN

