## COMPENG 4DM4 Assignment 1 Report

Aaron Pinto pintoa9 Raeed Hassan hassam41

October 24, 2022

## Exercise Part (A) - The 7-stage RISC Pipeline

- (A1) There is a 2 clock-cycle stall on LOAD instructions when the instruction following a LOAD instruction uses the value being loaded. The timing diagram can be seen in Figure 1.
- (A2) The number of branch-delay-slots following a BRANCH instruction will be 2 clock cycles in both cases considered:
- 1. If the value R0 being tested is available in a register at the start of the ID stage, then the "branch is resolved" in the ID stage the ID stage will compare R0 with zero, and generate a "Take-Branch" signal which is sent back to the IF1 stage from the ID stage in clock-cycle 3. In this case, 2 branch-delay-slots will occur, as seen in Figure 2. The compiler can attempt to fill the "BRANCH+1" and "BRANCH+2" branch delay slots with useful instructions, otherwise fill with a NO-OP.
- 2. If the value R0 is being computed in the EX stage, by the previous instruction, and R0 needs to be forwarded to the ID stage, then we do not "stretch the clock" to allow R0 to be tested in the ID stage in the same clock cycle. The system will "stall" the BNEZ for 1 extra clock cycle, waiting for R0 to be computed and forwarded to the ID stage. In this case, 2 branch-delay-slots will occur, as seen in Figure 3. The compiler can attempt to fill the "BRANCH+1" and "BRANCH+2" branch delay slots with useful instructions, otherwise fill with a NO-OP.

				Clock	Cycle										
Instruction	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
LW R0,0(R1)	IF1	IF2	ID	EX	MEM1	MEM2*	WB				*forwar	d R0 (M	EM2* to	*EX) in	сс6
ADD R3,R0,R2		IF1	IF2	ID	stall	stall	*EX	MEM1	MEM2	WB					
LOAD+2			IF1	IF2	stall	stall	ID	EX	MEM1	МЕМ2	WB				
LOAD+3				IF1	stall	stall	IF2	ID	EX	МЕМ1	MEM2				
LOAD+4					stall	stall	IF1	IF2	ID	EX	MEM1	MEM2			

Figure 1: Timing Diagram for A1

				Clock	Cycle							
Instruction	1	2	3	4	5	6	7	8	9	10	11	12
BNEZ R0, loop	IF1	IF2	ID*	EX	MEM1	МЕМ2	WB		*forwar	d R0 (ID	* to *IF1	) in cc
BRANCH+1		IF1	IF2	ID	EX	MEM1	МЕМ2	WB				
BRANCH+2			IF1	IF2	ID	EX	МЕМ1	МЕМ2	WB			
BRANCH TARGET				*IF1	IF2	ID	EX	МЕМ1	MEM2	WB		

Figure 2: Timing Diagram for A2 Case 1

				Clock	Cycle								
Instruction	1	2	3	4	5	6	7	8	9	10	11	12	13
previous instruction	IF1	IF2	ID	EX*	МЕМ1	МЕМ2	WB	*forwa	d R0 (E	X* to *ID	) in cc4		
BNEZ R0, loop		IF1	IF2	stall	*ID**	EX	MEM1	МЕМ2	WB	**forwa	rd R0 (II	D** to **I	F) in cc
BRANCH+1			IF1	stall	IF2	ID	EX	МЕМ1	МЕМ2	WB			
BRANCH+2				stall	IF1	IF2	ID	EX	MEM1	МЕМ2	WB		
BRANCH TARGET						**IF1	IF2	ID	EX	MEM1	МЕМ2	WB	

Figure 3: Timing Diagram for A2 Case 2

## Exercise Part (B) - Generate RISC Code for The Chacha20 Stream Cipher

- (B1) The unoptimized RISC code for the first 3 lines of the QUARTER-ROUND operation is shown in Listing 1. The following assumptions are made for this RISC code:
  - ASSUMPTION 1: assume that register R0 contains the address of the first word of the block of the initial key-stream
  - ASSUMPTION 2: each word is 32 bits, so use LD and SD instead of LW and SD to load 32-bit words
  - ASSUMPTION 3: words in the initial key-stream are stored consecutively in memory, address of second word is address of first world + 4 (bytes)

Listing 1: Unoptimized RISC code for the first 3 lines of QUARTER-ROUND operation

```
2
   \#define Ra \Rightarrow R1; Rb \Rightarrow R2; Rd \Rightarrow R3
                                                  % define Ra, Rb, Rd
3
4
   LD
             Ra, (0) R0
                               % load a from memory
   LD
             Rb, (16) R0
                               % load b from memory
6
   ADD
             Ra, Ra, Rb
                               \% a = a + b
7
                               \% store a in memory
   SD
             (0)R0,Ra
8
   LD
9
             Ra, (0) R0
                               % load a from memory
10
   LD
             Rd, (48) R0
                               % load d from memory
11
   XOR
             Rd, Rd, Rd
                               % XOR(d,a)
   SD
                               % store d in memory
12
             (48) R0, Rd
13
   LD
                               % load d from memory
14
             Rd, (48) R0
   ROT.L
             Rd, Rd, #16
                               % ROTATELEFT(d, 16)
15
16
   SD
             (48) R0, Rd
                               % store d in memory
```