Chapter 6 What's this Stuff on the Left?

Objectives

Upon completion of this chapter you will be able to:

- Describe the SI instruction format as used with the MVI and CLI instructions,
- Describe the ss instruction format as used with the MVC and CLC instructions,
- Describe the RX instruction format as used with the BC instruction,
- Given a partial .PRN with source code, determine the missing object code, and
- Given a partial . PRN with object code, determine the missing source code.

Introduction

We will now spend some time looking at the assembly listing in detail. For PC/370, this is the .prn file produced by A370. Our purpose in doing so is to get a better understanding of the assembly process, and to learn about instruction types. Such knowledge is important for debugging purposes. We will even learn to "reverse assemble" a program; that is, given some object code, determine the source instructions.

Each instruction has an instruction type. So far, we have looked at five instructions in detail: MVI, MVC, CLI, CLC, and BC. (Recall that all of the various branch instructions are variations of the BC instruction.) Macros, such as WTO and GET, consist of multiple instructions: they will not be discussed here. Consider the following (admittedly nonsensical) program, STUFF6A.MLC, which uses these instructions:

```
STUFF6A BEGIN
          CLC
                A,B
          ВL
          MVC
                C,B
                E,C'1'
          MVI
D
          EQU
                B,C'D'
          CLI
          ΒE
          MVC
                C,A
                E,C'9'
          MVI
F
          EQU
          RETURN
                CL3'AB'
Α
          DC
          DC
                 CL4'CDEF'
В
С
          DS
                CL2
                CL1'*'
Ε
          DC
          END
```

The following page shows the assembly (.PRN) listing for this program. Those portions of the program which we wish to concentrate on have been shaded (we ignore macro expansions.)

	STUFF6 PC/370	SA CROSS ASSEMBI	LER OPTIC	NS=L	KACE		PAGE	1
	LOC 000000 000000		ADR1	ADR2	1	LABEL *+++++ STUFF6A	-	OPERANDS
	000004		21.40	0058	3 4 5		USING B DC	*,15 KZHQX001 AL1(11)
	000010	E2E3E4C6C6F6C			6 7	HZQKX001	DC DC	CL11'STUFF6A ' 18F'0'
		90ECD00C 50D0F014		000C 0014	8 9	KZHQX001	STM ST	14,12,12(13) 13,HZQKX001+4
	000060	18ED 41D0F010		0010	10 11		LR LA	14,13 13,HZQKX001
		50D0E008		0008	12 13		ST DROP	13,8(0,14) 15
į	00006A				14		USING	HZQKX001,13
		D502D08ED091 4740D072	009E	00A1 0082	15 16		CLC BL	A,B D
		D201D095D091	00A5	00A1	17		MVC	C,B
		92F1D097 47F0D084		00A7 0094	18 19		MVI B	E,C'1' F
	000082	05045001	00000082	0071	20	D	EQU	*
		95C4D091 4780D084		00A1 0094	21 22		CLI BE	B,C'D' F
		D201D095D08E 92F9D097	00A5	009E 00A7	23 24		MVC MVI	C,A E,C'9'
	000094	921 900 97	00000094	UUA /	25		EQU	*
	000094	58DD0004		0004		*+++++	RETURN L	13,4(13)
		98ECD00C		000C	28 29		LM BR	14,12,12(13) 14
	00009E	C1C240			30		DC	CL3'AB'
	0000A1	C3C4C5C6			31 32		DC DS	CL4'CDEF'
	0000A7	5C			33		DC	CL1'*'
	8A0000				34		END	

The MVI and CLI instructions are type SI instructions, the MVC and CLC instructions are type SS instruction, and the BC instruction is a type RX instruction. These instruction types are commonly illustrated as follows:

	-	1	Lst Ha	alfwo	ord	2nd	d Halfwor	rd	3rc	d Hai	lfwor	d
Ì	SI	Op	Code		2	B ₁	D ₁					
Ì	SS*	Op	Code	I		B ₁	D ₁		B ₂		D ₂	- 1
Ì	RX	q0	Code	IR ₁	X ₂	B ₂	l D ₂					т

^{*} There is more than one form of SS instruction. This is the one we will look at for now...

CHAPTER 6 WHAT'S THIS STUFF ON THE LEFT?

where: Op Code. Operation code

B1, B2. Base register designation field

D1, D2 . . Displacement field

12 . . . Immediate operand field

L . . . Length field

x2 . . . Index Register designation field

Notice that *all* instructions use one, two, or three halfwords. Recall that a fullword is four bytes, so a halfword is two bytes. Therefore, *all* instructions occupy two, four, or six bytes.

The SI Instruction Format

All instructions which use the SI, or Storage Immediate, instruction format occupy two halfwords, or four bytes, as shown in the above illustration.

The first of these four bytes is the operation code, or Op Code. Each assembler instruction is assigned a decimal value from 0 to 255, just as are letters and numbers. An instruction may even have the same decimal value as a letter or number! For example, CLI is Op Code x'95', which is the same as a lower case 'n', and MVI is Op Code x'92', which is the same as a lower case 'k'. The CPU can tell the difference by the context in which it is encountered. Look at our sample program, a portion of which is repeated here. You can see the Op Codes of 95 and 92.

00006A	D502D08ED091	009E	00A1	15	CLC	А,В
000070	4740D072		0082	16	BL	D
000074	D201D095D091	00A5	00A1	17	MVC	С,В
00007A	92F1D097		00A7	18	MVI	E,C'1'
00007E	47F0D084		0094	19	В	F
000082		00000082		20 D	EQU	*
000082	95C4D091		00A1	21	CLI	B,C'D'
000086	4780D084		0094	22	BE	F
A80000	D201D095D08E	00A5	009E	23	MVC	C, A
000090	92F9D097		00A7	24	MVI	E,C'9'
000094		00000094		25 F	EOU	*

The second byte is the immediate value. In the case of the MVI and CLI instructions, the value to be moved or compared is actually a part of the instruction! For example, in line 18, we want to move a '1' to field E. The EBCDIC equaivalent to a '1' is decimal 241 or hex F1, and you can see that F1 is part of the instruction; immediately following the Op Code of 92. Similarly, in line 21, we want to check to see if the first byte of field B is the letter D. The EBCDIC equivalent to a 'D' is decimal 196, or hex C4, and you can see that C4 is part of the instruction; immediately following the Op Code of 95.

The next part, **base** and **displacement**, is a bit more confusing, but it is something you *must* understand if you are to be successful with assembly language. The next halfword of the instruction indicates the address of the first operand; the field to be moved to or compared to. Within those two bytes, the first half-byte (that's four bits only, or one hex digit) indicates the base register. Recall from our discussion of binary numbers that four bits could range in value from 0 (0000, or all bits off) to 15 (1111, or all bits on). This is also the range of registers: we have sixteen registers, numbered from 0 to 15 inclusive. So these four bits designate a register. In all three of the above instructions (lines 18, 21, and 24), the next half-byte (following the immediate value) is D, which is the hex equivalent to decimal 13. This says that register 13 is pointing to the operands, or close to them. How can this be? Where did we so initialize register 13? We didn't, but the BEGIN macro uses register 13 as the **base register**. This is done by the USING instruction in line 14, which is part of the expansion of the BEGIN macro. Register 13 points to HZQKX001 (a nonsensical label generated by the BEGIN macro) which is the start of the program. The next one and one-half bytes (that's twelve bits) indicate the displacement, or distance, of the operand from HZQKX001.

In line 18, the displacement is x'097'. The address of HZQKX001 is X'000010' (in the LOC column at line 7 of the program). So if we add X'097' to X'000010' we get X'0000A7', which is the LOC for field E!

In line 21, the displacement is x'091'. The address of HZQKX001 is X'000010' (in the LOC column at line 7 of the program). So if we add X'091' to X'000010' we get X'0000A1', which is the LOC for field B!

The assembler will save us some of this work. Where approriate, the assembler will place the address of operands in columns ADR1 or ADR2. For example, in line 18, where we wish to move '1' to field E, ADR2 is 00A7, same as we found by adding the displacement to the base. Likewise, in line 21, where we wish to check to see if the first byte of field B is the letter D, ADR2 is 00A1, same as we found above.

Clearly the ADR1 and ADR2 columns are easier to use. So why learn the other way? Because when we are looking at object code only, such as during a test session or when debugging, the ADR1 and ADR2 columns will not be available.

You Try It...

- 1. Show the object code for line 18 if that line were changed to MVI E, C'2'
- 2. Show the object code for line 21 if that line were changed to CLI B+1, C'\$'
- 3. Show the object code for line 24 if that line were changed to MVI E+1, X'40'

The SS Instruction Format

	+				-+-				-+-				-+
		1st	Hal	fword		2nc	l Hal	fword		3rd	Hal:	fword	
+-	 -+		+-		-+-	+			-+-	+			-+
				L									
Τ-	 					7			-T				- +

All instructions which use the ss, or Storage-to-Storage, instruction format occupy three halfwords, or six bytes, as shown in the above illustration.

As with all assembler instructions, the first of these six bytes is the operation code, or Op Code. CLC is Op Code x'D5' (same as an upper case 'N') and MVC is Op Code x'D2' (same as an upper case 'K'). Look at our sample program, a portion of which is repeated here. You can see the Op Codes of D5 and D2.

00006A D	502D08ED091	009E	00A1	15	CLC	A,B
000070 47	740D072		0082	16	BL	D
000074 D2	201D095D091	00A5	00A1	17	MVC	C,B
00007A 92	2F1D097		00A7	18	MVI	E,C'1'
00007E 47	7F0D084		0094	19	В	F
000082		00000082		20 D	EQU	*
000082 95	5C4D091		00A1	21	CLI	B,C'D'
000086 47	780D084		0094	22	BE	F
00008A D2	201D095D08E	00A5	009E	23	MVC	C,A
000090 92	2F9D097		00A7	24	MVI	E,C'9'
000094		00000094		25 F	EQU	*

The second byte is the length of the operation. Recall that a single byte can range in value from 0 to 255. But a move of length 0 doesn't make any sense. So the length operand is actually the length of the operation *minus one*. In this way, values from 0 to 255 indicate operation lengths (moves, compares, etc.) of from 1 to 256 inclusive. This is why the MVC and CLC instructions are limited to 256 characters.

In line 15, we compare field $\mathbb A$ with field $\mathbb B$. Field $\mathbb A$ is defined as 3 bytes long, whereas field $\mathbb B$ is defined as 4 bytes long. Recall from our discussion of the CLC instruction that the length of the compare is determined by the length of the first operand. Since that operand, field $\mathbb A$, is 3 bytes long, 3 bytes will be compared. This is shown in the instruction as 3 *minus one*, or 2. The hex representation of 2 is $\times 1021$, and that is what follows the op code; that is, a CLC for a length of 3 is represented as $\times 105021$.

In line 17, we move field B to field C. Field B is defined as 4 bytes long, whereas field C is defined as 2 bytes long. We know that the length of an MVC is determined by the length of the first operand. Since that operand, field C, is 2 bytes long, 2 bytes will be compared. This is shown in the instruction as 2 *minus one*, or 1. The hex representation of 1 is X'01', and that is what follows the op code; that is, an MVC for a length of 2 is represented as X'D201'.

The second halfword (third and fourth bytes) indicates the base and displacement of the first operand, and the third halfword (fifth and sixth bytes) indicates the base and displacement of the second operand. These work the same as described in the SI format instruction above, except that there are two operands instead of one. Our earlier discussion of the ADR1 and ADR2 columns applies as well.

You Try It...

- 4. Show the object code for line 15 if that line were changed to CLC B, A
- 5. Show the object code for line 15 if that line were changed to CLC A+1(2), B+2
- 6. Show the object code for line 23 if that line were changed to MVC C(3), B

The RX Instruction Format

All instructions which use the RX, or Register-Index, instruction format occupy two halfwords, or four bytes, as shown in the above illustration.

Again, the first of these four bytes is the operation code. BC is Op Code X'47'. Look at our sample program: you can see the Op Code of 47.

00006A	D502D08ED091	009E	00A1	15	CLC	A , B	
000070	4740D072		0082	16	BL	D	
000074	D201D095D091	00A5	00A1	17	MVC	С,В	
00007A	92F1D097		00A7	18	MVI	E,C'1'	
00007E	47F0D084		0094	19	В	F	
000082		00000082		20 D	EQU	*	
000082	95C4D091		00A1	21	CLI	B,C'D'	
000086	4780D084		0094	22	BE	F	
00008A	D201D095D08E	00A5	009E	23	MVC	C,A	
000090	92F9D097		00A7	24	MVI	E,C'9'	
000094		00000094		25 F	EQU	*	

The next half-byte (four bits) corresponds to the mask. The value of this mask, which ranges from 0000 (all bits off) to 1111 (all bits on), is determined by the mnemonic (BE, BL, etc.) and corresponds to the possible values of the condition code which we discussed in an earlier chapter. For example, we said that if we were comparing two fields, A and B, and A was less than B, the resulting condition code would be 01002, or x'4'. In line 16 above, we want to branch to D if A is less than B. So the mask is x'4', which you see immediately after the op code of x'47'.

The next half-byte indicates the index register. An index register is like a displacement

whose value depends upon a register. Whereas the other displacements we looked at were constant, the value of the register, and hence the total displacement, may vary. When the index

register is 0, it is ignored. This will usually be the case. In all of the above branches, the index

We have seen that a BL is shown as X'4740', a B (unconditional) as X'47F0', and a BE as X'4780'. For completeness, we show the following table:

BE	X'4780'
BH	X'4720'
BL	X'4740'
BNE	X'4770'
BNH	X'47D0'
BNL	X'47B0'
В	X'47F0'

As before, the second half word of the instruction gives the base and displacement of the label to which the instruction should branch. The only difference between this and the $\mathfrak{s}\mathfrak{l}$ and $\mathfrak{s}\mathfrak{s}$ instruction formats which we have discussed is that, again, there is an index register which allows for a second level of displacement.

You Try It...

register is zero.

- 7. Show the object code for line 16 if that line were changed to BH D
- 8. Show the object code for line 19 if that line were changed to B
- 9. Show the object code for line 22 if that line were changed to BNE F

Data Definition Instructions

Finally, we turn our attention to the data definition instructions, DS and DC.

00009E C1C240	30 A	DC	CL3'AB'
0000A1 C3C4C5C6	31 B	DC	CL4'CDEF'
0000A5	32 C	DS	CL2
0000A7 5C	33 E	DC	CL1'*'

As you can see, when a DS instruction is used, no object code is generated: the left side of the listing is blank. However, the location counter is incremented. For example, field C begins at location 0000A5, for a length of two. Therefore, the next field (E) will begin at location 0000A5 + 0002 = 0000A7.

When a DC instruction is used, the hexadecimal representation of the data is shown. If the field is over eight bytes in length, the first eight bytes (only) are shown. As with the DS instruction, the location counter is incremented. For example, field A begin at location ODDODE, for a length of

three. Therefore, the next field will begin at location 00009E + 0003 = 0000A1. Field A is initialized

three. Therefore, the next field will begin at location 00009E + 0003 = 0000A1. Field A is initialized to C'ABb', which is shown as X'C1C240'. X'40' is a blank: memorize that!

You Try It...

- 10. Show the object code for line 30 if that line were changed to A DC CL3'A'
- 11. Show the object code for line 31 if that line were changed to B DC CL4'12'
- 12. Show the object code for line 33 if that line were changed to E DC 2X'FE'

- 1. True or false.
 - T F a. The MVI and MVC instructions are of type ss.
 - F b. Every instruction occupies exactly one, two, or three halfwords.
 - T F C. The second byte of an MVI instruction contains the length of the move, minus one.
 - T F d. Register 13 is our base register, as indicated by the BEGIN macro.
 - T F e. If the first operand of an MVC is indicated by X'DO10', then the target (receiving) field begins ten bytes past where register 13 is pointing.
 - T F f. If the length of a CLC is indicated by X'OC', then twelve bytes are being compared.
 - T F g. The Op Code for BE and BNE are both X'47'.
 - T F h. Given E DC C'B', the stuff on the left will be X'C2'.
 - T F i. Given F DC CL2'B', the stuff on the left will be x'C2C2'.
 - T F j. X'4708' is the object code for BC with a mask of 8.
 - T F k. Given A DS CL3 at LOC=0000AE, then A+2 is at LOC=0000B0.
 - T F l. Given R DS CL1, the stuff on the left will be X'D9'.
 - T F m. The base register designator (B_1 or B_2) occupies one byte of object code.
- 2. Given MVI D, C'B' generated 92C2D08A at LOC=0000BC, and D is defined as CL3.
 - a. What is the LOC for the next instruction?
 - b. Show the object code if this line were changed to MVI D, C'C'
 - c. Show the object code if this line were changed to MVI D+1,C'D'
 - d. Show the object code if this line were changed to MVI D+2, X'DD'
 - e. Show the object code if this line were changed to CLI D, C'E'
 - f. Show the object code if this line were changed to CLI D+1, B'11100010'
- 3. Given MVC X, Y generated D20AD090D080 at LOC=0000D6, and Y is defined as CL14.
 - a. How long is x?
 - b. What is the LOC for the next instruction?
 - c. Show the object code if this line were changed to MVC X(4), Y
 - d. Show the object code if this line were changed to MVC X+2 (5), Y
 - e. Show the object code if this line were changed to MVC X+3(1), Y+4
 - f. Show the object code if this line were changed to MVC Y, X
 - g. Show the object code if this line were changed to CLC X, Y
 - h. Show the object code if this line were changed to CLC Y(3), X+1

4. a. Fill in the blanks (lines 15-21 and 27):

STUFF	6B					PAGE	1
PC/370	CROSS ASSEMBI	LER OPTIC	ONS=L	KACE			
LOC		ADR1	ADR2	LINE	LABEL	OP	OPERANDS
000000				1	*+++++	BEGIN	
000000				2	STUFF6B	CSECT	
000000				3		USING	* , 15
000000	47F0F058		0058	4		В	KZHQX001
000004	0B			5		DC	AL1(11)
000005	E2E3E4C6C6F60	2240		6		DC	CL11'STUFF6B '
000010	000000000000000000000000000000000000000	0000		7	HZQKX001	DC	18F'0'
000058	90ECD00C		000C	8	KZHQX001	STM	14,12,12(13)
00005C	50D0F014		0014	9		ST	13,HZQKX001+4
000060	18ED			10		LR	14,13
	41D0F010		0010	11		LA	13,HZQKX001
	50D0E008		8000	12		ST	13,8(0,14)
00006A				13		DROP	15
00006A				14		USING	HZQKX001,13
	D201D086D088	0096	0098	15		MVC	, Y
	92F9D08D		009D	16		MVI	Z,,Y
	95D3D086		0096	17		CLI	
	4780D07C		008C	18			W
	D501D086D08D	0096	009D	19			X, Z
	4740D07C		008C	20		BL	
	D203D08DD088	009D	0098	21			, Y
00008C		0000008C		22		EQU	*
00008C				23	*+++++		
	58DD0004		0004	24		L	13,4(13)
	98ECD00C		000C	25		LM	14,12,12(13)
000094	07FE			26		BR	14
	D1D2			27		DC	CL2''
	D3D4D5D6D7			28		DC	CL5'LMNOP'
	D8D9E2E3			29	Z	DC	CL4'QRST'
0000A8				30		END	

b. You be the computer...what are the values of x, y, and z after this program runs?

X =	Y=	=	Z	=

5. a. Fill in the blanks (lines 15-19 and 25-27):

STUFF6	5C					PAGE	1
PC/370	CROSS ASSEMBI	LER OPTIC	NS=L	KACE			
LOC		ADR1	ADR2	LINE	LABEL	OP	OPERANDS
000000				1	*+++++	BEGIN	
000000				2	STUFF6C	CSECT	
000000				3		USING	* , 15
000000	47F0F058		0058	4		В	KZHQX001
000004	0B			5		DC	AL1(11)
000005	E2E3E4C6C6F60	C340		6		DC	CL11'STUFF6C '
000010	000000000000000000000000000000000000000	0000		7	HZQKX001	DC	18F'0'
	90ECD00C		000C	8	KZHQX001	STM	14,12,12(13)
	50D0F014		0014	9		ST	13, HZQKX001+4
	18ED			10		LR	14,13
	41D0F010		0010	11		LA	13,HZQKX001
	50D0E008		0008	12		ST	13,8(0,14)
00006A				13		DROP	15
00006A				14		USING	HZQKX001,13
00006A	D07CD07A	008C	008A	15		CLC	D,F
000070	D06C		007C	16		BL	H
000074	D07D		008D	17		MVI	E,C'D'
000078	D070		0800	18		В	G
00007C	D07C		008C	19		MVI	D,C'F'
080000		080000080		20	G	EQU	*
080000				21	*++++++	RETURN	
080000	58DD0004		0004	22		L	13,4(13)
000084	98ECD00C		000C	23		LM	14,12,12(13)
000088				24	_	BR	14
A80000				25		DC	
00008C					D	DC	
00008D	C6C5C4			27	E	DC	
000090				28		END	

b.	You be the computerwhat are the values of F , D , and E after this program
	runs?

F=	D=	E=

6. a. Fill in the blanks (lines 15-19):

STUFF6	5D					PAGE	1
PC/370 CROSS ASSEMBLER OPTIONS=LXACE							
LOC		ADR1	ADR2	LINE	LABEL	OP	OPERANDS
000000				1	*+++++	BEGIN	
000000				2	STUFF6D	CSECT	
000000				3		USING	* , 15
	47F0F058		0058	4		В	KZHQX001
000004				5		DC	AL1(11)
	E2E3E4C6C6F60			6		DC	CL11'STUFF6D '
	000000000000000000000000000000000000000	0000		7	HZQKX001	DC	18F'0'
000058	90ECD00C		000C	8	KZHQX001	STM	14,12,12(13)
	50D0F014		0014	9		ST	13,HZQKX001+4
000060				10		LR	14,13
	41D0F010		0010	11		LA	13,HZQKX001
	50D0E008		0008	12		ST	13,8(0,14)
00006A				13		DROP	15
00006A				14		USING	HZQKX001,13
			008D	15		MVI	M,C'L'
		A800	008D	16		MVC	L(2),M
			008A	17		CLI	L,C'N'
			0800	18		BNE	N
			008A	19		MVI	L,C'M'
080000		0800000			N	EQU	*
080000				21	*++++++	RETURN	
	58DD0004		0004	22		L	13,4(13)
	98ECD00C		000C	23		LM	14,12,12(13)
000088				24		BR	14
A80000					L	DC	CL3'MOM'
00008D	4040			26	M	DC	CL2' '
000090				27		END	

b. You be the computer...what are the values of ${\tt L}$ and ${\tt M}$ after this program runs?

L=	M=
----	----

7. a. Fill in the blanks (lines 15-19 and 25-27):

STUFF	δE					PAGE	1
PC/370	CROSS ASSEMBI	LER OPTIC	ONS=L	KACE			
LOC		ADR1	ADR2	LINE	LABEL	OP	OPERANDS
000000				1	*+++++	BEGIN	
000000				2	STUFF6E	CSECT	
000000				3		USING	* , 15
000000	47F0F058		0058	4		В	KZHQX001
000004	0B			5		DC	AL1(11)
000005	E2E3E4C6C6F60	C540		6		DC	CL11'STUFF6E '
000010	000000000000000000000000000000000000000	0000		7	HZQKX001	DC	18F'0'
	90ECD00C		000C	8	KZHQX001	STM	14,12,12(13)
	50D0F014		0014	9		ST	13,HZQKX001+4
	18ED			10		LR	14,13
	41D0F010		0010	11		LA	13,HZQKX001
	50D0E008		8000	12		ST	13,8(0,14)
00006A				13		DROP	15
00006A				14		USING	HZQKX001,13
	D501D07FD081	008F	0091	15	P		
	4720D072		0082	16			
	D201D081D07C	0091	008C	17			
	92F2D081		0091	18			
	47F0D05A		006A	19			
000082		00000082		20	Q	EQU	*
000082				21	*++++++	RETURN	
	58DD0004		0004	22		L	13,4(13)
000086	98ECD00C		000C	23		LM	14,12,12(13)
A80000				24	_	BR	14
	F1F2F3			25			
00008F				26	S		
000091	F3F3			27	R		
000098				28		END	

b.	You be the computerwhat are the values of T, S, and R after this program
	runs?

T=	S=	R=