Appendix A – Logs and Antilogs for Galois Field 256

In GF(256), each number can be represented by $\alpha^n (0 \le n \le 255)$. Ex:

$$1 = \alpha^0$$
$$2 = \alpha^1$$
$$4 = \alpha^2$$
$$8 = \alpha^3$$
$$16 = \alpha^4$$
$$32 = \alpha^5$$
$$64 = \alpha^6$$
$$128 = \alpha^7$$

The above part is the same as the polynomial representation mentioned in Section III. E (1). As the power goes larger, we need to apply multiplication rule to calculate the number:

$$\alpha^8 = \alpha^8 \ mod \ P(\alpha)$$

Remember that the number representation of α^8 is 256 (9'b100000000), and $P(\alpha) = \alpha^8 + \alpha^4 + \alpha^3 + \alpha^2 + 1$ is 285 (9'b100011101), the modulo operation can be achieved by XOR logic (Since the subtraction is same as XOR in GF(256)):

$$\alpha^8 = \alpha^8 \ mod \ P(\alpha) = 256 \text{ XOR } 285 = 29$$

$$\begin{array}{r|l} & 1 \\ \hline \alpha^8 + \alpha^4 + \alpha^3 + \alpha^2 + 1 & \alpha^8 \\ & \alpha^8 + \alpha^4 + \alpha^3 + \alpha^2 + 1 \\ \hline & \alpha^4 + \alpha^3 + \alpha^2 + 1 = 29 \end{array} \quad \Rightarrow \quad \left.\begin{array}{r} 1\,0\,0\,0\,0\,0\,0\,0\,0\,(256) \\ 1\,0\,0\,0\,1\,1\,1\,0\,1\,(285) \end{array}\right\} XOR \atop \overline{0\,0\,0\,0\,1\,1\,1\,0\,1\,(29)}$$

Fig. A.1 This figure shows why a modulo operation is equal to the XOR logic.

We can find the number with higher power by the similar method:

$$\alpha^9 = \alpha^8 \times \alpha = 29 \times 2 = 58$$

$$\alpha^{10} = \alpha^9 \times \alpha = 58 \times 2 = 116$$

$$\alpha^{11} = \alpha^{10} \times \alpha = 116 \times 2 = 232$$

$$\alpha^{12} = \alpha^{11} \times \alpha = 232 \times 2 = 464 \ XOR \ 285 = 205$$

The full table of GF (256) from α^0 to α^{255} can be found in the attached excel file "log_antilog.xlsx".

Appendix B – The Error Correction Steps for Rank B Test Pattern 00

The codewords of Rank B test pattern 00 are:
[64,247,116,7,114,230,230,70,71,82,230,86,71,82,231,71,112,236,17,236,17,236,17,236,17,236,17,236,229,84,149,108,126,123,9,11,50,193,94,112,219,217,206,109]

If you decode directly without error correction, the decoded text will be "w@w.nddu.edu.tw". The true text should be "www.nthu.edu.tw", with the codewords below:
[64,247,119,119,114,230,231,70,135,82,230,86,71,82,231,71,112,236,17,236,17,236,17,236,17,236,17,236,229,84,149,108,126,123,9,11,50,193,94,112,219,217,206,109]

Let us run the error correction steps to get the correct codewords.
First, convert the error codewords to α^n notation:
$[\alpha^6, \alpha^{232}, \alpha^{10}, \alpha^{198}, \alpha^{155}, \alpha^{160}, \alpha^{160}, \alpha^{48}, \alpha^{253}, \alpha^{148}, \alpha^{160}, \alpha^{219}, \alpha^{253}, \alpha^{148}, \alpha^{81}, \alpha^{253}, \alpha^{202}, \alpha^{122}, \alpha^{100}, \alpha^{122}, \alpha^{100}, \alpha^{122}, \alpha^{100}, \alpha^{122}, \alpha^{100}, \alpha^{122}, \alpha^{100}, \alpha^{122}, \alpha^{169}, \alpha^{143}, \alpha^{184}, \alpha^{250}, \alpha^{167}, \alpha^{172}, \alpha^{223}, \alpha^{238}, \alpha^{194}, \alpha^{45}, \alpha^{70}, \alpha^{202}, \alpha^{177}, \alpha^{96}, \alpha^{111}, \alpha^{133}]$

Next, calculate the syndrome:

$$S_0 = R(1) = \alpha^6\ XOR\ \alpha^{232}\ XOR\ \alpha^{10}\ \text{XOR} \ldots\ldots \text{XOR}\ \alpha^{111}\ \text{XOR}\ \alpha^{133} = \alpha^{211}$$
$$S_1 = R(\alpha) = (\alpha^6 \times \alpha^{43}) XOR (\alpha^{230} \times \alpha^{42}) XOR \ldots\ldots XOR\ \alpha^{133} = \alpha^{244}$$
$$S_2 = R(\alpha^2) = (\alpha^6 \times \alpha^{86}) XOR (\alpha^{230} \times \alpha^{84}) XOR \ldots\ldots XOR\ \alpha^{133} = \alpha^{246}$$
$$S_3 = R(\alpha^3) = (\alpha^6 \times \alpha^{129}) XOR (\alpha^{230} \times \alpha^{126}) XOR \ldots\ldots XOR\ \alpha^{133} = \alpha^{100}$$
$$S_4 = R(\alpha^4) = (\alpha^6 \times \alpha^{172}) XOR (\alpha^{230} \times \alpha^{168}) XOR \ldots\ldots XOR\ \alpha^{133} = \alpha^{62}$$
$$S_5 = R(\alpha^5) = (\alpha^6 \times \alpha^{215}) XOR (\alpha^{230} \times \alpha^{210}) XOR \ldots\ldots XOR\ \alpha^{133} = \alpha^{60}$$
$$S_6 = R(\alpha^6) = (\alpha^6 \times \alpha^{3}) XOR (\alpha^{230} \times \alpha^{252}) XOR \ldots\ldots XOR\ \alpha^{133} = \alpha^{139}$$
$$S_7 = R(\alpha^7) = (\alpha^6 \times \alpha^{46}) XOR (\alpha^{230} \times \alpha^{39}) XOR \ldots\ldots XOR\ \alpha^{133} = \alpha^{136}$$

Then, solve $\sigma_4, \sigma_3, \sigma_2, \sigma_1$ for:

$$\alpha^{211}\sigma_4 - \alpha^{244}\sigma_3 + \alpha^{246}\sigma_2 - \alpha^{100}\sigma_1 + \alpha^{62} = 0 \quad \cdots\cdots\cdots (Eq1)$$
$$\alpha^{244}\sigma_4 - \alpha^{246}\sigma_3 + \alpha^{100}\sigma_2 - \alpha^{62}\sigma_1 + \alpha^{60} = 0 \quad \cdots\cdots\cdots (Eq2)$$
$$\alpha^{246}\sigma_4 - \alpha^{100}\sigma_3 + \alpha^{62}\sigma_2 - \alpha^{60}\sigma_1 + \alpha^{139} = 0 \quad \cdots\cdots\cdots (Eq3)$$
$$\alpha^{100}\sigma_4 - \alpha^{62}\sigma_3 + \alpha^{60}\sigma_2 - \alpha^{139}\sigma_1 + \alpha^{136} = 0 \quad \cdots\cdots\cdots (Eq4)$$

By elimination method, we can choose any two of the four equations above to eliminate σ_4. Repeat this step three times, we can get Eq5, Eq6, and Eq7 with just three unknown variables ($\sigma_3, \sigma_2, \sigma_1$). Then, again, we can choose any two of the three equations (Eq5, Eq6, Eq7) to eliminate σ_3. Repeat two times, we can get Eq8 and Eq9 with just two unknown variables (σ_2, σ_1).

For example, multiply α^{33} to Eq1 and then add Eq1 and Eq.2 together, we can get Eq.5:

$$(\alpha^{244}\ XOR\ \alpha^{244})\sigma_4 - (\alpha^{22}\ XOR\ \alpha^{246})\sigma_3 + (\alpha^{24}\ XOR\ \alpha^{100})\sigma_2$$
$$-(\alpha^{133}\ XOR\ \alpha^{62})\sigma_1 + (\alpha^{95}\ XOR\ \alpha^{60}) = 0$$

Which means:

$$-\alpha^{36}\sigma_3 + \alpha^{137}\sigma_2 - \alpha^{171}\sigma_1 + \alpha^{92} = 0 \quad \cdots\cdots\cdots (Eq5)$$

With same approach, we can get Eq6 from Eq2 and Eq3, and Eq7 from Eq3 and Eq4:

$$-\alpha^{51}\sigma_3 + \alpha^{146}\sigma_2 - \alpha^{160}\sigma_1 + \alpha^{35} = 0 \quad \cdots\cdots\cdots (Eq6)$$
$$-\alpha^{6}\sigma_3 + \alpha^{197}\sigma_2 - \alpha^{96}\sigma_1 + \alpha^{34} = 0 \quad \cdots\cdots\cdots (Eq7)$$

After getting Eq5, Eq6, and Eq7, we can then get Eq8 from Eq5 and Eq6, and Eq9 from Eq6 and Eq7:

$$\alpha^{82}\sigma_2 - \alpha^{103}\sigma_1 + \alpha^{230} = 0 \quad \cdots\cdots\cdots (Eq8)$$
$$\alpha^{142}\sigma_2 - \alpha^{233}\sigma_1 + \alpha^{250} = 0 \quad \cdots\cdots\cdots (Eq9)$$

With Eq8 and Eq9, we can start calculating σ_1 by multiplying α^{60} to Eq8, and then add Eq8 and Eq9 together:

$$(\alpha^{142}\ XOR\ \alpha^{142})\sigma_2 - (\alpha^{163}\ XOR\ \alpha^{233})\sigma_1 + (\alpha^{35}\ XOR\ \alpha^{250}) = 0$$

Which means:

$$-\alpha^{227}\sigma_1 + \alpha^{79} = 0$$

Then:

$$\sigma_1 = \alpha^{107}$$

Substitute σ_1 into Eq8, and we can get:

$$\alpha^{82}\sigma_2 - \alpha^{103+107} + \alpha^{230} = 0, \text{then } \sigma_2 = \alpha^{170}$$

With σ_1 and σ_2, we can substitute them into Eq5. to get σ_3:

$$-\alpha^{36}\sigma_3 + \alpha^{137+170} - \alpha^{171+107} + \alpha^{92} = 0, \text{then } \sigma_3 = \alpha^{63}$$

With σ_1, σ_2 and σ_3, we can substitute them into Eq1. to get σ_4:

$$\alpha^{211}\sigma_4 - \alpha^{244+63} + \alpha^{246+170} - \alpha^{100+107} + \alpha^{62} = 0, \text{then } \sigma_4 = \alpha^{153}$$

After getting $\sigma_4, \sigma_3, \sigma_2, \sigma_1$, we can calculate the error location by finding the solution i such that:

$$\sigma(\alpha^i) = \alpha^{153} + \alpha^{63}\alpha^i + \alpha^{170}\alpha^{2i} + \alpha^{107}\alpha^{3i} + \alpha^{4i} = 0$$

In this example, i has four solutions: [35, 37, 40, 41].

As mentioned earlier, the solution $i = [35, 37, 40, 41]$ means the error occurred at codeword 8, 6, 3 and 2, which is the same as the red marked codewords in page 2.

Finally, we are calculating the offset of error by solving Y_1, Y_2, Y_3, Y_4 for:

$$Y_1(\alpha^{35})^1 + Y_2(\alpha^{37})^1 + Y_3(\alpha^{40})^1 + Y_4(\alpha^{41})^1 = \alpha^{211}$$
$$Y_1(\alpha^{35})^2 + Y_2(\alpha^{37})^2 + Y_3(\alpha^{40})^2 + Y_4(\alpha^{41})^2 = \alpha^{244}$$
$$Y_1(\alpha^{35})^3 + Y_2(\alpha^{37})^3 + Y_3(\alpha^{40})^3 + Y_4(\alpha^{41})^3 = \alpha^{246}$$
$$Y_1(\alpha^{35})^4 + Y_2(\alpha^{37})^4 + Y_3(\alpha^{40})^4 + Y_4(\alpha^{41})^4 = \alpha^{100}$$

Using the same method to solve the four-unknown equations, we can get:

$$Y_1 = \alpha^{251}, Y_2 = \alpha^{218}, Y_3 = \alpha^{162}, Y_4 = \alpha^{239}$$

And the error offsets are:

$$Y_1\alpha^{i_1} = \alpha^{251} \times \alpha^{35} = \alpha^{31} = 192$$
$$Y_2\alpha^{i_2} = \alpha^{218} \times \alpha^{37} = \alpha^{255} = 1$$
$$Y_3\alpha^{i_3} = \alpha^{162} \times \alpha^{40} = \alpha^{202} = 112$$
$$Y_4\alpha^{i_4} = \alpha^{239} \times \alpha^{41} = \alpha^{25} = 3$$

The final step is to correct the error by the position and offset we've calculated:

Correct position 35 (codeword 8):

$$135 \text{ XOR } 192 = 71$$

Correct position 37 (codeword 6):

$$231 \text{ XOR } 1 = 230$$

Correct position 40 (codeword 3):

$$119 \text{ XOR } 112 = 7$$

Correct position 41 (codeword 2):

$$119 \text{ XOR } 3 = 116$$

And we can get the corrected codewords to decode the correct text.

Appendix C – JIS8 code table [1]

Char.	Hex	Char.	Hex	Char.	Hex	Char.	Hex	Char.	Hex	Char.	Hex	Char.	Hex	Char.	Hex
NUL	00	SP	20	@	40	`	60		80		A0	ﾀ	C0		E0
SOH	01	!	21	A	41	a	61		81	｡	A1	ﾁ	C1		E1
STX	02	"	22	B	42	b	62		82	｢	A2	ﾂ	C2		E2
ETX	03	#	23	C	43	c	63		83	｣	A3	ﾃ	C3		E3
EOT	04	$	24	D	44	d	64		84	､	A4	ﾄ	C4		E4
ENQ	05	%	25	E	45	e	65		85	･	A5	ﾅ	C5		E5
ACK	06	&	26	F	46	f	66		86	ｦ	A6	ﾆ	C6		E6
BEL	07	'	27	G	47	g	67		87	ｧ	A7	ﾇ	C7		E7
BS	08	(	28	H	48	h	68		88	ｨ	A8	ﾈ	C8		E8
HT	09	)	29	I	49	I	69		89	ｩ	A9	ﾉ	C9		E9
LF	0A	*	2A	J	4A	j	6A		8A	ｪ	AA	ﾊ	CA		EA
VT	0B	+	2B	K	4B	k	6B		8B	ｫ	AB	ﾋ	CB		EB
FF	0C	,	2C	L	4C	l	6C		8C	ｬ	AC	ﾌ	CC		EC
CR	0D	-	2D	M	4D	m	6D		8D	ｭ	AD	ﾍ	CD		ED
SO	0E	.	2E	N	4E	n	6E		8E	ｮ	AE	ﾎ	CE		EE
SI	0F	/	2F	O	4F	o	6F		8F	ｯ	AF	ﾏ	CF		EF
DLE	10	0	30	P	50	p	70		90	ｰ	B0	ﾐ	D0		F0
DC1	11	1	31	Q	51	q	71		91	ｱ	B1	ﾑ	D1		F1
DC2	12	2	32	R	52	r	72		92	ｲ	B2	ﾒ	D2		F2
DC3	13	3	33	S	53	s	73		93	ｳ	B3	ﾓ	D3		F3
DC4	14	4	34	T	54	t	74		94	ｴ	B4	ﾔ	D4		F4
NAK	15	5	35	U	55	u	75		95	ｵ	B5	ﾕ	D5		F5
SYN	16	6	36	V	56	v	76		96	ｶ	B6	ﾖ	D6		F6
ETB	17	7	37	W	57	w	77		97	ｷ	B7	ﾗ	D7		F7
CAN	18	8	38	X	58	x	78		98	ｸ	B8	ﾘ	D8		F8
EM	19	9	39	Y	59	y	79		99	ｹ	B9	ﾙ	D9		F9
SUB	1A	:	3A	Z	5A	z	7A		9A	ｺ	BA	ﾚ	DA		FA
ESC	1B	;	3B	[	5B	{	7B		9B	ｻ	BB	ﾛ	DB		FB
FS	1C	<	3C	¥	5C	|	7C		9C	ｼ	BC	ﾜ	DC		FC
GS	1D	=	3D	]	5D	}	7D		9D	ｽ	BD	ﾝ	DD		FD
RS	1E	>	3E	^	5E	‾	7E		9E	ｾ	BE	ﾞ	DE		FE
US	1F	?	3F	_	5F	DEL	7F		9F	ｿ	BF	ﾟ	DF		FF

Note that the codes 8'h00-8'h7f are the same as those in the ASCII code.

Appendix D – Test pattern list

Pat no	Orientation	Top-left corner location	Mask	Text length	Text	Error text
00	0	(36, 0)	6	15	www.nthu.edu.tw	w@w.nddu.edu.tw
01	0	(39, 17)	1	17	www.wikipedia.org	wwG.wiklpodia#org
02	0	(16, 18)	2	17	www.google.com.tw	www.geegle.com.tn
03	0	(31, 36)	3	13	goo.gl/rYWrb4	goo.gl?rZWrd5
04	0	(38, 21)	0	13	goo.gl/w8z8rb	goo.gl/w7zirb
05	0	(6, 25)	4	24	Galois Field is amazing!	Galoes field is amazing?
06	0	(24, 10)	5	23	2'b11 XOR 2'b10 = 2'b01	2'b11 NOR 3'b10 = 2'b11
07	0	(0, 22)	3	24	assign enable=(Z>B)?1:0;	bssign enable!(X>B)?1:0;
08	0	(27, 8)	7	25	ICLab homework 4 is easy!	ICLab homework 4 is hard?
09	0	(11, 35)	2	22	ncverilog -f gatesim.f	ncverylon -v gatesim.v
10	90	(7, 8)	6	15	www.nthu.edu.tw	w@w.nddu.edu.tw
11	90	(12, 1)	1	17	www.wikipedia.org	wwG.wiklpodia#org
12	90	(36, 15)	2	17	www.google.com.tw	www.geegle.com.tn
13	90	(0, 18)	3	13	goo.gl/rYWrb4	goo.gl?rZWrd5
14	90	(28, 33)	0	13	goo.gl/w8z8rb	goo.gl/w7zirb
15	90	(39, 2)	4	24	Galois Field is amazing!	Galoes field is amazing?
16	90	(15, 23)	5	23	2'b11 XOR 2'b10 = 2'b01	2'b11 NOR 3'b10 = 2'b11
17	90	(26, 39)	3	24	assign enable=(Z>B)?1:0;	bssign enable!(X>B)?1:0;
18	90	(19, 30)	7	25	ICLab homework 4 is easy!	ICLab homework 4 is hard?
19	90	(35, 29)	2	22	ncverilog -f gatesim.f	ncverylon -v gatesim.v
20	180	(34, 32)	6	15	www.nthu.edu.tw	w@w.nddu.edu.tw
21	180	(31, 16)	1	17	www.wikipedia.org	wwG.wiklpodia#org
22	180	(27, 22)	2	17	www.google.com.tw	www.geegle.com.tn
23	180	(2, 5)	3	13	goo.gl/rYWrb4	goo.gl?rZWrd5
24	180	(15, 8)	0	13	goo.gl/w8z8rb	goo.gl/w7zirb
25	180	(11, 39)	4	24	Galois Field is amazing!	Galoes field is amazing?
26	180	(35, 21)	5	23	2'b11 XOR 2'b10 = 2'b01	2'b11 NOR 3'b10 = 2'b11
27	180	(0, 9)	3	24	assign enable=(Z>B)?1:0;	bssign enable!(X>B)?1:0;
28	180	(20, 10)	7	25	ICLab homework 4 is easy!	ICLab homework 4 is hard?
29	180	(0, 39)	2	22	ncverilog -f gatesim.f	ncverylon -v gatesim.v
30	270	(39, 6)	6	15	www.nthu.edu.tw	w@w.nddu.edu.tw
31	270	(4, 24)	1	17	www.wikipedia.org	wwG.wiklpodia#org
32	270	(26, 12)	2	17	www.google.com.tw	www.geegle.com.tn

33	270	(37, 33)	3	13	goo.gl/rYWrb4	goo.gl?rZWrd5
34	270	(11, 27)	0	13	goo.gl/w8z8rb	goo.gl/w7zirb
35	270	(15, 16)	4	24	Galois Field is amazing!	Galoes field is amazing?
36	270	(25, 31)	5	23	2'b11 XOR 2'b10 = 2'b01	2'b11 NOR 3'b10 = 2'b11
37	270	(17, 5)	3	24	assign enable=(Z>B)?1:0;	bssign enable!(X>B)?1:0;
38	270	(7, 39)	7	25	ICLab homework 4 is easy!	ICLab homework 4 is hard?
39	270	(29, 38)	2	22	ncverilog -f gatesim.f	ncverylon -v gatesim.v