Analysis of the Galois Iterator PhL 8.29.13

I added the results of these notes as best I could to the Observations section of Section 3.2 item 6.

The goal here is to interpret all stuff related to my "Galois iterator".

From Section 2.2 we had these equations

$$q'(x) = x\,q(x) - o\,h(x) + i \quad . \qquad (2.2.4)$$

$$\{q'(x)\} = \{x\}\bullet\{q(x)\} - \{o\}\bullet\{h(x)\} + \{i\} \quad .$$

$$\{q'(x)\} = \{x\}\bullet\{q(x)\} + \{i\} \quad . \qquad (2.2.13)$$

$$\alpha = \{x\} \qquad \beta = \{q(x)\} \qquad \beta' = \{q'(x)\} \qquad \{i\} = i\{1\} = i\,1 \quad . \qquad (2.2.14)$$

$$\beta' = \alpha\bullet\beta + i1 = \alpha\beta + i\,1 \quad .$$

$$\beta_{s+1} = \alpha\,\beta_s + i_s\,1 \quad . \qquad (2.2.15)$$

$$\beta_s = \alpha^s\,\beta_0 + [\,\alpha^{s-1}\,i_0 + \alpha^{s-2}\,i_1 + \ldots + \alpha\,i_{s-2} + i_{s-1}\,]\,1 \qquad (2.2.16)$$

Discussion: The first equation comes right from the circuit where q(x) is a polynomial whose coefficients are the register values. Thus q(x) is a remainder polynomial and its coefficients are a k-tuple representation of a GF(p^k) field element. I say $\beta = \{q(x)\}$ in the sense of abstract β corresponds to this particular remainder under division by h(x). The association $\alpha = \{x\}$ makes α be a primitive element since h(x) is a prim poly and $h(\{x\}) = h(\alpha) = 0$ which I do state somewhere. The equals sign in $\beta = \{q(x)\}$ represents an isomorphism of some sort as I show somewhere in GA, it is not a true equality. Here is a triple association which does not yet include my matrix thing:

a_i	$\doteq$	$\{\,r_i(x)\,\}$	$\doteq$	$r_i(x) = \mathrm{Rem}(f_i^{(k)}(x)/d(x))$	(10.2)
abstract field element		chart row		remainder polynomial	

Then later I include the matrix

α	$\doteq$	$\{\,x\,\}$	$=$	x	$\doteq$	X	(10.8)
primitive abstract field element		chart row		remainder polynomial		matrix representation	

Question: Given some q(x) remainder, what is the corresponding matrix Q ?

Answer: This has to come from the enumeration table for GF(p^k). The first powers are simple

X^0 $\{1\} = 00001$

X^1 $\{x\} = 00010$

X^2 $\{x^2\} = 00100$

etc

For example, for GF(2^3) I show that

Table for GF(2^3)	$\alpha^7 = 1$	(6.9) m=3 $\alpha^3 = \alpha + 1$	(6.10) m=3 $\alpha^n = A_2\alpha^2 + A_1\alpha + A_0$

n	α^n	A_2	A_1	A_0	hex		
1	α^1	0	1	0	2		
2	α^2	1	0	0	4		
3	α^3	0	1	1	3	// $\alpha + 1$	
4	α^4	1	1	0	6	// $\alpha^2 + \alpha$	
5	α^5	1	1	1	7	// $\alpha^2 + \alpha + 1$	
6	α^6	1	0	1	5	// $\alpha^2 + 1$	
7,0	α^7	0	0	1	1	// 1	(6.12)

so in this case we can look up any q(x) in the m-tuple $A_2..A_0$ columns and see what X^n power it matches. For example, q(x) = 101 = $x^2 + 1$ corresponds to X^6. So at least I think I know how to go back and forth between power of the matrix X and the m-tuple representation

So basically in Section 2.2 I start with a physical equation from the actual circuit which involves polys and I apply the special {...} operation to convert this to an abstract Galois field equation involving things like α and β and β_s where s is just a time subscript (why didn't I use n for that? Well, I was using n as the order of α at that time.

There are no bolded vectors in this section 2.2. There are only q(x) polynomials, but of course that does imply a vector.

From Section 3.2 I again start with the physical circuit and I quickly come up with

$$\begin{vmatrix} q'_1 \\ q'_2 \\ q'_3 \\ q'_4 \\ \dots \\ q'_{k-1} \\ q'_k \end{vmatrix} = \begin{vmatrix} 0 & 0 & 0 & \dots & 0 & -h_0 \\ 1 & 0 & 0 & \dots & 0 & -h_1 \\ 0 & 1 & 0 & \dots & 0 & -h_2 \\ 0 & 0 & 1 & \dots & 0 & -h_3 \\ & & & \dots & & \\ 0 & 0 & 0 & \dots & 0 & -h_{k-2} \\ 0 & 0 & 0 & \dots & 1 & -h_{k-1} \end{vmatrix} \begin{vmatrix} q_1 \\ q_2 \\ q_3 \\ q_4 \\ \dots \\ q_{k-1} \\ q_k \end{vmatrix} + \begin{vmatrix} i \\ 0 \\ 0 \\ 0 \\ .. \\ 0 \\ 0 \end{vmatrix} \qquad (3.2.2)$$

Now we can write this in compact vector/matrix notation as:

$$\mathbf{q'} = B\,\mathbf{q} + i\,\mathbf{1} \qquad (3.2.3)$$

For the first time, I now have bolded vectors which represent GF(p^k) elements in the k-tuple basis. And I also have the matrix B which is my primitive element. Compare

$$\mathbf{q'} = B\ \mathbf{q} + i\,\mathbf{1} \qquad \text{matrix/vector form} \qquad (3.2.3)$$

$q'(x) = x\,q(x) - o\,h(x) + i\ .$ physical equation in terms of polys *(2.2.4)*

$\{q'(x)\} = \{x\} \bullet \{q(x)\} + i\{1\}$ remainder form (2.2.13)

$\beta' = \alpha \bullet \beta + i1$ abstract form

$\alpha = \{x\} \qquad \beta = \{q(x)\} \qquad \beta' = \{q'(x)\} \qquad \{i\} = i\{1\} = i\,1\ .$ (2.2.14)

What is unusual here is that in the lower two forms, all Galois elements are of the same "type": they are all remainders, or they are all "abstract field elements". But in the first form, B is a matrix while **q** is a k-tuple so the field elements are on a different footing. This is just the way things come out and it is rather handy.

I want to say that in this matrix/vector form we have

B = a primitive element of GF(p^k) in a matrix representation of GF(p^k)
q = an element of GF(p^k) in a k-tuple representation of GF(p^k) associated with poly coeffs

Suppose **q** = (0,0...0,1,0) meaning q(x) = x. In this case we know that **q** = B in our equivalence equality and then we have

$\mathbf{q'} = B\ \mathbf{q} + i\ \mathbf{1}$

$= B\ B + i\ I = B^2 + i\,I$ = some matrix element of GF(p^k).

OK, I think I need to modify the Observations following (3.2.5). AT least this is the section where I need to say whatever it is I want to say.

OK, stop. I have done my best adding notes to the Observation section of scrambler doc Sec 3.2. It is just some weird mixed representation of the abstract Galois equation. I don't think there is more that one can say. At least I how have some "words" in there about this strange equation.