Old Fact 7 and Fact 8 from Section 2.3 PhL 6.28.13

It turned out that Fact 7 as shown below is wrong, and I used it to prove Fact 8. Here are the original and invalid Facts 7 and 8 just for safe keeping:

****

Fact 7: If the integer n happens to be the *period* of h(x), then at least n solutions of the difference equation (2.3.2) have period n. (2.3.11)

Proof: We already know from Fact 6 (2.3.10) that the period of any solution must divide n. The question here is whether there are some solutions which have the full period n.

Consider the code word c(x) obtained by multiplying the generator g(x) by unity. We claim that this **c** has the full period n. To show this, assume first that it does not, and that it has some smaller period m = n/N. In this case we must be able to group the elements of **c** into N identical groups of m symbols. In this case we can write:

$$c(x) = g(x) = f(x) [\ 1 + x^m + x^{2m} + x^{3m} + ... + x^{(N-1)m}\ ]$$

where f(x) is a polynomial of degree m representing the pattern that repeats N times. We recognize the above [...] as $(x^n - 1) / (x^m - 1)$ where n = Mm. And of course $(x^n - 1) = g(x)h(x)$ as usual. Thus we have

$$g(x) = f(x)\,(x^n - 1) / (x^m - 1) = f(x)g(x)h(x) / (x^m - 1)\ .$$

Cancelling g(x) we find that $f(x)h(x) = (x^m - 1)$ where m<n . But by definition, assuming that the *period* of h(x) is n means there is no such m < n such that h(x) divides $(x^m - 1)$. Thus we arrive at a contradiction, so it must be that this c(x) = g(x) has the full period n, and therefore the corresponding solution to the difference equation (2.3.2) must have the full period n as well.

Furthermore, we know we can form n-1 distinct other code words by taking cyclic permutations of this g(x) code word, and all of these code words will have period n as well. QED

How do we know that ?

Fact 8: If h(x) of degree k is a *primitive polynomial* of $GF(p^k)$, then *all* $p^k - 1$ non-zero solutions of the difference equation (2.3.2) have period $P = p^k - 1$. (2.3.12)

Proof: This is the big result we have been waiting for. The proof is so simple that it is deceptive. From GA (5.10), we know that if h(x) is a primitive polynomial of $GF(p^k)$, then h(x) has period $n = p^k - 1$. From Fact 7 above, we know that in this case we can produce n solutions of the difference equation (2.3.2) which have the full period n -- these are just the n cyclic permutations of the code word g(x) filled out with zeros to have n coefficients, as illustrated in the Example above.

On the other hand, from the discussion following Fact 3, we know that the cyclic code generated by g(x) has exactly p^k code words. One of these is the zero code word, so this leaves $p^k - 1$ non-zero code words. But this is n just quoted above. We know from Fact 5 that every solution of (2.3.2) corresponds to

a code word. Since there are n non-zero code words, there are only n non-zero solutions, and we have found them all, and they all have period $n = p^k - 1$.

****

Here are the NEW Fact 7 and Fact 8, now installed in scrambler doc:

Fact 7: If h(x) is a primitive polynomial of GF(q), then no code word c(x) has a period less than $n \equiv q-1$. In other words, since c(x) corresponds to **c** which has n components $c = \{c_1, c_2 .... c_n\}$, this Fact is saying that the set of components cannot be partitioned into a repeating set of subsequences such as **c** = {a,b,a,b....a,b}.

Proof: Suppose c(x) has a period m = n/M for some integer M > 1. In other words, suppose **c** consists of an integral number M>1 of repeating subsequences. From GA Chap 8 (k) we know that if h(x) is a primitive polynomial, then all non-zero code words c(x) are rotations of g(x) which is one of the code words. Suppose then that **c** had a repeating subsequence of components, for example

$c(x) \sim \{abcde\ abcde\ abcde\}$.

Suppose g(x) were a rotation of one symbol left relative to c(x). Then we would have

$g(x) \sim \{bcde\ abcde\ abcde\ a\} = \{bcdea\ bcdea\ bcdea\}$.

For a rotation of some general number of symbols we would get

$g(x) \sim \{ABCDE\ ABCDE\ ABCDE\}$.

Then g(x) must have a repeating subsequence of period m. If this is so, we can write

$$g(x) = f(x) [\ 1 + x^m + x^{2m} + x^{3m} + ... + x^{(M-1)m}\ ]$$

where f(x) is a polynomial of degree m representing the pattern that repeats M times. But we know that

$$[1 + y + y^2 + ... + y^{s-1}\ ] = (y^s - 1)/(y-1)$$

so setting $y = x^m$ and $s = M-1$ we find that

$$[\ 1 + x^m + x^{2m} + x^{3m} + ... + x^{(M-1)m}\ ] = (x^{Mm} - 1)/(y-1) = (x^n - 1)/(x^m-1)$$

and therefore

$$g(x) = f(x)\ (x^n - 1)/(x^m-1)\ .$$

But since $(x^n - 1) = g(x)h(x)$ this says

$$g(x) = f(x)\, g(x)h(x)/(x^m-1)$$

or

$$1 = f(x)\, h(x)/(x^m-1)\ .$$

This says that h(x) integrally divides (x^m-1) with $m < n$, but when h(x) is a primitive polynomial, we know that the lowest power m must be n. Therefore we arrive at a contradiction, so g(x) cannot have a repeating subsequence and since all other code words are rotations of g(x), they cannot have repeating subsequences either.

Example: In Example B above we found that **c** = {1,1,1,1,0,1,0,1,1,0,0,1,0,0,0} is a code word. Notice that this cannot be partitioned into a set of repeating subsequences. The same is then true for all the other code words shown in Example B, since they are rotations of **c**.

Now here is my new Fact 8

Fact 8: If h(x) of degree k is a primitive polynomial of $GF(p^k)$, then *all* $p^k - 1$ non-zero solutions of the difference equation (2.3.2) have period $P = p^k - 1$. (2.3.12)

Proof: We know from Fact 7 that, when h(x) is a primitive polynomial, the period of any code word c(x) is $n = q-1 = p^k-1$. From Fact 4, all $p^k - 1$ solution sequences $\{o_i\}$ have the form $\{o_i\} = \{\mathbf{c},\mathbf{c},\mathbf{c},\mathbf{c}\ ...\}$. Thus all these solutions have period n.