Paradox with (8.22) PhL 7.7.13

I had a big confusion regarding (8.21) and nearby because I seemed to get the cyclic property of code words *without* using g(x) must divide x^n-1. This has all been resolved and the section updated.

Definition: The **FACT**: g(x) must divide x^n-1 as part of cyclic code definition.

Paradox: In my first derivation that a cyclic code is cyclic, I must use the FACT. But in my alternate derivation (8.22), the FACT is not needed. How can this be?

I agree that this is a mysterious section of my doc just in general, but I tried to be as careful as possible.

1. Look again at Math Lemma 1 of (8.15).

Only assumption here is f(x) has degree n-1 (so it could be a code word). I show that

$$xf(x) = [\, f^{(1)}(x)\,] + f_{n-1}(x^n - 1) \quad \text{where } f^{(1)}(x) \text{ has degree } n-1$$

so that

$$xf(x)/(x^n - 1) = f_{n-1} + [\, f^{(1)}(x)\,]/(x^n - 1)$$

This says that

$$\text{Rem}[xf(x)/(x^n - 1)] = f^{(1)}(x)$$

This really is a remainder because the fraction $[\, f^{(1)}(x)\,]/(x^n - 1)$ is degree n-1 over degree n. So I see nothing wrong with this math lemma.

2. Look again at Math Lemma 2.

It is just an iteration of Lemma 1, I do not see the FACT in use here, but I do see (x^n-1) appearing.

3. Fact 5 proof:

Lemma 2 with c(x) as the poly. Assume c(x) = g(x)d(x). Then use the FACT. Only with the FACT do we get the form $c^{(m)}(x) = [\, x^m d(x) - q(x)h(x)\,]\, g(x)$ so that g(x) is factored out leaving [...]. Then I claim that the degree of [...] must be $\leq$ k-1 so $d_m(x)$ must be a data word and then $c^{(m)}(x)$ must be a code word. I had to use the FACT to get the factorization which made this fly.

4. The ring A_n (now to section (g))

R_q is polys with coefficients in GF(q), a bit unusual in my stuff, perhaps important. So the A_n think must be all polys over GF(q) which are remainders of degree < n. Why am I using R_q here instead of my simpler R thing? Remainders have coeffs in R_q then. There are q*q*q...*q = q^n such remainders. First

paragraph under (8.18) seems OK. I have d(x) c(x) and g(x) I guess with coeffs in GF(q). I agree that all of d(x),g(x) and c(x) are somewhere in this A_n chart. I agree to (8.19) as {..} property for any res class ring deal. I agree with (8.20).

I think Fig 7.8 is perfect and quite a good picture in retrospect. The sea of (.) comment is good too.

5. Now consider Fact 6 which is (8.21)

Warning: {a}{b} = {c} does not imply that ab = c.

I know at once that c(x) = d(x)g(x) so yes, all code words are multiples of g(x), but that is not enough to say that the code words are an ideal in A_n. We have to show this to be true, the ideal part. Let's study my ideal proof now. Ideal within A_n is the issue. The {c(x)} code word remainders are in A_n and I think this is an additive group closed under addition. Lets make sure

$$\{c_1(x)\} + \{c_2(x)\} = \{ c_1(x) + c_2(x)\} = \{c_3(x)\}$$

So I think the remainders {c(x)} are closed under addition.

I have to show this thing {r(x)}•{c(x)} is some $\{c_1(x)\}$ and this is true for any {c} in (g) and for any r at all. So I start off

$$\{r(x)\}\bullet\{c(x)\} = \{r(x)\}\bullet\{g(x)d(x)\} = \{r(x)g(x)d(x)\} = \{r(x)d(x)\} \bullet \{g(x)\}$$

I need to show somehow that

$$\{r(x)d(x)\} \bullet \{g(x)\} = \{c_1(x)\} \qquad ?$$

If I knew that r(x)d(x) was a data poly, then I think it would be shown, but even that is a maybe.

Lemma: Consider {d'}{g} = {c} which says {d'g}={c}. If d is degree < k (and of course g has degree =n-k) then we know that d'g has degree < n and THEN we can conclude that d'g = c. But we MUST know that d' has the right degree to be a data poly.

So why should r(x)d(x) be a data poly for arbitrary r and d ? It is NOT a data poly. But can we show that

$$\{ r(x)d(x)\} = \{d_1(x)\} \quad \text{where } d_1 \text{ IS a data poly?}$$

We would have to show that

$$r(x)d(x) /(x^n-1) = q(x) + d_1(x)/ (x^n-1)$$

which is to say

$$r(x)d(x) = q(x) (x^n-1) + d_1(x)$$

Well, this is all valid, but all you know is that d_1 has degree < n. This is not good enough. Now suppose we add in our FACT at this point. Then we can say

$$r(x)d(x) = q(x)\, g(x)\, h(x) + d_1(x)$$

and then

$$[r(x)d(x)]/h(x) = q(x)\, g(x) + d_1(x)/h(x)$$

and NOW you can conclude that d_1 has degree < k. So you need the FACT!!!!

Without this fact, I think we conclude that {c(x)} is NOT an ideal in A_n . So Fact 6 is then not valid.

Now continue to (8.22) Fact 5 Revisited and show how this proof fails.

Proof: Here we are giving an "alternate proof" of Fact 5 (8.17). Actually, it is the same proof as above, only here it is expressed in the language of rings and ideals.

A code word c(x) is a polynomial of degree < n. Thus, according to Math Lemma 2 (8.16),

$$c^{(m)}(x) = \text{Rem}[\, (x^m\, c(x))/\, (x^n - 1)] \,,$$

where $c^{(m)}(x)$ is a cyclic permutation of c(x) by m places. Since c(x) is of degree < n, we know that $\{ c(x) \} \in A_n$. If m < n, then $\{ x^m \} \in A_n$. Thus, we can rewrite the above equation as

$$\{ c^{(m)}(x) \} = \{ x^m \} \bullet \{ c(x) \} \,. \qquad \text{(has } q^n \text{ rows)}$$

? r i

Because {c(x)} is an element of the ideal (g(x)), and because $\{ x^m \} \in A_n$, it follows from the definition of an ideal that $\{ c^{(m)}(x) \}$ is also in the ideal (g(x)). Thus, $\{ c^{(m)}(x) \}$ must be some code word. **QED**.

OK, I have found it, lets fix it!

********** attempted new proof **********

Fact 6: The chart rows {c(x)} form an *ideal* (g(x)) within A_n. (8.21)

In other words, the code word polynomials of a cyclic code comprise an ideal within the set of polynomials of degree < n. We shall denote this ideal as (g(x)), meaning rows { f(x) } of A_n where f(x) is any multiple of g(x).

Proof: Here we use "code word" to refer to the polynomial associated with a code word.

An ideal I of a ring R was defined in (1.22). Certainly the set {c(x)} is a subgroup of A_n under the + operation, since the sum of any two code words is a code word (recall that C^k is a vector space). We then have to show that r•I = I. This means that {r(x)}•{i(x)} = {i'(x)} for any {r(x)} in A_n and any {i(x)} in the ideal (g(x)). Since our candidate ideal is I = {c(x)}, the set of code words, i(x) is some code word,

call it c(x). We then have to show that {r(x)}•{c(x)} = {c'(x)} where c'(x) is some other code word, where r(x) is some arbitrary element of A_n.

The proof that {c(x)} is an ideal is slippery and one can easily go astray. We know that c(x) = d(x)g(x) for some d(x) so we want to show that

{r(x)}•{ d(x)g(x)} = {c'(x)} ? // for any r(x) in R_q so any {r(x)} in A_n

or

{r(x)d(x)}•{g(x)} = {c'(x)} ? // for any r(x) in R_q so any {r(x)} in A_n

If we knew that {r(x)d(x)} = {d_1(x)} for some data d_1(x) (degree < k), we could write the left side as

{r(x)d(x)}•{g(x)} = {d_1(x)}•{g(x)} = {d_1(x)g(x)} = {c_1(x)}

where $c_1(x) \equiv d_1(x)g(x)$ is a code polynomial, and then our proof that {c(x)} is an ideal would be concluded with c' = c_1. But we *don't* know that such a d_1(x) exists with degree < k. What we do know is this:

$r(x)d(x) /(x^n-1) = q(x) + d_2(x)/ (x^n-1)$ =>

{r(x)d(x)} = {d_2(x)} where $d_2(x)$ has degree < n.

This is not good enough to obtain the proof. Extra information is required. From the second line back we can write

$r(x)d(x) = q(x) (x^n-1) + d_2(x)$.

Now the "extra information required" is the fact that g(x) divides x^n- 1 so that $(x^n-1) = g(x)h(x)$ where recall g(x) has degree n-k and h(x) has degree k. Then we have

$r(x)d(x) = q(x) g(x) h(x) + d_2(x)$

Since $d_2(x)$ can have degree ≥ k, in full generality we can expand it as

$d_2(x) = Q(x)h(x) + d_3(x)$ where $d_3(x)$ has degree < k .

Then the second equation previous reads

$r(x)d(x) = [q(x) g(x) + Q(x)] h(x) + d_3(x)$

This proof is not working. !!! I did show why my previous one failed, but I now need a new proof that works to replace it.

****

Fact 6: The chart rows {c(x)} form an *ideal* (g(x)) within A_n. (8.21)

In other words, the code word polynomials of a cyclic code comprise an ideal within the set of polynomials of degree < n. We shall denote this ideal as (g(x)), meaning rows { f(x) } of A_n where f(x) is any multiple of g(x).

Proof: An ideal I of a ring R was defined in (1.22). First of all, the set {c(x)} is an additive subgroup of A_n, as required. The set contains the additive identity 0 from c(x) = 0 and the other required properties including closure under + :

$\{c_1(x)\} + \{c_2(x)\} = \{c_1(x) + c_2(x)\} = \{c_3(x)\}$ // closed under A_n + operation

We then have to show that r•I = I. This means that {r(x)}•{i(x)} = {i'(x)} for any {r(x)} in A_n and any {i(x)} in the ideal (g(x)). Since our candidate ideal is I = {c(x)}, the set of code word polynomials, i(x) is some code word polynomial, call it c(x). We then have to show that {r(x)}•{c(x)} = {c'(x)} where c'(x) is some other code word polynomial, where r(x) is some arbitrary element of A_n. Setting c(x) = d(x)g(x), this is what we need to show

{r(x)}•{ d(x)g(x)} = {c'(x)} . where c'(x) is a code word polynomial

Here is a proof pathway that looks promising, but does not succeed. Rewrite the above as

{r(x)d(x)}•{g(x)} = {c'(x)} .

If we knew that {r(x)d(x)} = $\{d_1(x)\}$ for some data $d_1(x)$ (degree < k), we could write the left side as

{r(x)d(x)}•{g(x)} = $\{d_1(x)\}$•{g(x)} = $\{d_1(x)g(x)\}$ = $\{c_1(x)\}$

where $c_1(x) \equiv d_1(x)g(x)$ is a code word polynomial, and then our proof that {c(x)} is an ideal would be concluded with c' = c_1. But we *don't* know that such a $d_1(x)$ exists with degree < k, so this approach does not work.

Here is a viable proof. We know we can write

{r(x)}•{d(x)g(x)} = {f(x)}

where f(x) has degree < n and is the remainder of r(x)d(x)g(x) divided by x^n-1. But this does not tell us that f(x) is a code word. Now we add the assumption that g(x)h(x) = (x^n-1). Multiply both sides of the above equation by h(x) and rearrange

{r(x)d(x)} • {g(x) h(x)} = {f(x) h(x)}

or

{r(x)d(x)} • {x^n-1} = {f(x) h(x)}

or

$$\{r(x)d(x)\} \bullet \mathbf{0} = \{f(x)\ h(x)\}$$

or

$$\{f(x)\ h(x)\} = \mathbf{0}\ .$$

This says that

$$\text{Rem}\left[\frac{f(x)\ h(x)}{x^{n}-1}\right] = 0$$

or

$$f(x)h(x) = q(x)(x^{n}-1)\ .$$

$$<n\ \ k \qquad\qquad <k\ \ \ n$$

The degree of quotient q(x) must be < k in order to balance the powers on the two sides of this last equation. Therefore q(x) can be regarded as a data polynomial. Rewrite the above as

$$f(x)h(x) = q(x)g(x)h(x)$$

or

$$f(x) = q(x)g(x).$$

Since q(x) is a data polynomial, f(x) must be a code polynomial, QED.