**Saved Old Appendix B called 2.1** PhL 6.25.13

New version installed.

**Appendix 2.1: Proof of Fact 4 of Section 2.3**

First, we restate the thing we want to prove:

**Fact 4**: If **c** is any code word of the cyclic code generated by g(x), then the infinite sequence

$$\{o_i\} = \{\mathbf{c},\mathbf{c},\mathbf{c} \ldots\}$$

is a solution of the difference equation (2.3.2).

**Proof:**

This proof uses various results from Ref. GA. The reader is assumed to know the meaning of a linear block code and a dual code, for example.

(1) GA Section 7 (d) gives the following simple proof that the code words of any linear block code G are orthogonal to the code words of the dual code H,

$$\mathbf{c}' \bullet \mathbf{c}^T = (\mathbf{d}'\bullet H)\bullet(\mathbf{d}\bullet G)^T = (\mathbf{d}'\bullet H)\bullet G^T\bullet\mathbf{d}^T = \mathbf{d}'\bullet(H\bullet G^T)\bullet\mathbf{d}^T = \mathbf{d}'\bullet(0)\bullet\mathbf{d}^T = 0 \qquad \text{below GA (7.24)}$$

Recall that the T transpose symbol is present just to make one vector a column and the other a row, so we can dot them together. We could also write the above as

$$(\mathbf{c}')^T \bullet \mathbf{c} = 0 \ .$$

(2) GA Section 8 discusses cyclic codes. Certainly h(x) is a code word of the dual code of g(x). Code words are just multiples of their generator, and h(x) is a multiple of h(x) which is the generator of the code dual to that of the code generated by g(x). Thus, we can think of the coefficients of h(x) as the **c'** in the above equation. Of course h(x) has k coefficients, and we have then to add n-k zeros to make a true dual code vector **h**. Consider this done. Now, if **c** is any code word of the cyclic code generated by g(x), we have

$$\mathbf{h}^T \bullet \mathbf{c} = 0$$

If we write this out as a summation, we get

$$\sum_{j=0}^{k} h_j \ c_j = 0$$

where the numbers $\{c_0 , c_1, c_2, \ldots c_k\}$ are the first k coefficients of any code word of g(x).

We have just proved this fact:

**Fact** : The dot product of the coefficients of h with the first k+1 coefficients of any code word gives 0.

(3) What happens if we dot h with any k+1 consecutive coefficients of a code word **c**? We know that there is some other code word **c'** for which these k+1 consecutive coefficients are the *first* k+1 coefficients. We know this because we know that all cyclic permutations of code words are also code words. Thus we have proved that :

**Fact**: The dot product of the coefficients of h with any consecutive k+1 coefficients of any code word gives 0. Consecutive means in the cyclic sense, so that for example $c_{k-1}$ , $c_k$, $c_0$, $c_1$ are consecutive.

(4) Now consider what it *means* to show that an infinite sequence {o} is a solution of the difference equation (2.3.2)

$$\sum_{j=0}^{k} h_j \; o_{n+j} = 0 \qquad (2.3.2)$$

Picture the sequence $\{o_i\}$ as an infinite row of numbers. Picture the sequence $\{h_j\}$ as a finite row of numbers. Place the row $\{h_j\}$ anywhere under the infinite row $\{o_i\}$, then take the dot product of the abutting numbers. This is then the left side of (2.3.2), and the result is supposed to be zero. Varying n means varying the position of the row $\{h_j\}$. Here is a picture drawn for k=3, and n=5:

| $o_0$ | $o_1$ | $o_2$ | $o_3$ | $o_4$ | $o_5$ | $o_6$ | $o_7$ | $o_8$ | $o_9$ | $o_{10}$ | $o_{11}$ | ... |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | $h_0$ | $h_1$ | $h_2$ | $h_3$ | | | | |

Now consider our candidate solution of the difference equation:

$$\{o_i\} = \{\mathbf{c}, \mathbf{c}, \mathbf{c}, \mathbf{c} \ldots\}$$

Consider the above process. No matter where we position $\{h_j\}$, we will be dotting h with a consecutive set of k+1 coefficients of the code word **c**. We have just shown that this gives 0. Thus, $\{o_i\}$ = {**c**,**c**,**c**,**c**...} is a solution of the difference equation (2.3.2). **QED**