Note that page numbering is turned on in this template.

We know that h(x) divides into $x^{15} - 1$ to give g(x). We would like to find this g(x). Here is a hand calculation of g(x),

$h(x) = 1 + x + x^2 + x^3 + x^4 = (x^5 - 1) / (x-1)$

$g(x) = (x^{15} - 1) / h(x) = (x-1)\ [(x^{15} - 1) / (x^5 - 1)] = (x-1)\ (x^{10} + x^5 + 1)$

$g(x) = x^{11} - x^{10} + x^6 - x^5 + x - 1$

But since p = 2 in this example, GF(2) only has elements 0 and 1, and -1 = 1 so then

$g(x) = x^{11} + x^{10} + x^6 + x^5 + x + 1$.

Here is how Maple does the same computation,

```
h := 1 + x + x^2 + x^3 + x^4;
```

$$h := 1 + x + x^2 + x^3 + x^4$$

```
Quo(x^15-1,h,x) mod 2;
```

$$x^{11} + x^{10} + x^6 + x^5 + x + 1$$

What is the period of h(x) ?

Now we can write down some of the code words of the cyclic code generated by this g(x). This subject is summarized at the start of Appendix B. Our first code word is g(x) itself, and then we do all cyclic permutations. Notice for this g(x) code word we start at the right and then fill with three zeros on the left to get it from n-k to n coefficients. Please do not miss the point here. Code words are multiplies of g(x), so the unit multiple c(x) = g(x) is one of the code words

{ 1,1,0,0,0, 1,1,0,0,0, 1,1,0,0,0} $g(x) = x^{11} + x^{10} + x^6 + x^5 + x + 1$

We have artificially introduced gaps to reveal the repeating pattern that results.

Convention Note: There are two conventions for how to order coefficients. We are using the convention which puts the coefficient of the lowest power of the polynomial on the left. This is consistent with our statement for example that **c** = $\{c_0, c_1, c_2, c_3, c_4\}$ as in examples above. Perversely, we display g(x) with the lowest power on the right. Both these conventions are just the reverse of Peterson and Weldon as quoted in (2.2.22). In Ref. GA we use several notations to deal with this ambiguity,

$f(x) = a + bx + kx^3$ = <ab0k> = [k0ba] = k0ab now fixed in GA // = a 4-tuple GA (4.6)

but here we use {a,b,0,k} instead of <ab0k> .

We can do cyclic permutations on the above to get 5 of the 16 codes words.

{ 0,0,0,1,1,	0,0,0,1,1,	0,0,0,1,1}
{ 0,0,1,1,0,	0,0,1,1,0,	0,0,1,1,0}
{ 0,1,1,0,0,	0,1,1,0,0,	0,1,1,0,0}
{ 1,1,0,0,0,	1,1,0,0,0,	1,1,0,0,0}
{ 1,0,0,0,1,	1,0,0,0,1,	1,0,0,0,1}

Fig 2.2

To get the other code words, add two of the above and then take its 5 cyclic forms, and then add another two and get its 5 cyclic forms. The 16th code word is all zeros.

Now, construct a shift register generator with 4 registers and use $h(x) = 1 + x + x^2 + x^3 + x^4$. We know that all output sequences are of the form $\{o_i\} = \{\mathbf{c},\mathbf{c},\mathbf{c},\mathbf{c} \ldots\}$. Looking at the above code words, we quickly conclude that the period of all possible non-zero output streams is 5 !

This result is consistent with Fact 5 of Section 2.1. There, we showed that the state vector period of the shift register was equal to the order of the Galois element {x} which is a root of h(x). For our h(x) here, $\{x\} = \alpha^3$ which has order 5. Since the state vector repeats every 5 clocks, it is not too surprising that the output sequence has this same period.

Comment: GF(16 = 2^4) has exactly four minimum polynomials, two of which are primitive polynomials. They are all computed in GA and we quote them below. Primitive polynomials always occur in order reversed pairs as one sees in the first two items in the table which are denoted 10011 and 11001 :

$p_1(x)$	$= (x - \alpha)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8)$	$= x^4 + x + 1$
$p_7(x)$	$= (x - \alpha^7)(x - \alpha^{14})(x - \alpha^{13})(x - \alpha^{11})$	$= x^4 + x^3 + 1$
$m_3(x)$	$= (x - \alpha^3)(x - \alpha^6)(x - \alpha^{12})(x - \alpha^9)$	$= x^4 + x^3 + x^2 + x + 1$
$m_5(x)$	$= (x - \alpha^5)(x - \alpha^{10})$	$= x^2 + x + 1$ GA (6.21)

The ones in the Peterson and Weldon list above are p_1, m_3 and m_5.

• end of example