Appendix E: Existence of g(x) which divides $x^n - 1$.

In our definition (8.1) of a cyclic code, we required that generator g(x) divide $x^n - 1$ where n is the length of the (n,k) code. It was not required that n be the period of g(x), so n might not be the smallest s for which g(x) divides $x^s - 1$. Nor was it required that g(x) be irreducible. In particular, g(x) need not be the primitive polynomial of some Galois Field.

The purpose of this Appendix is to demonstrate that for any positive integer n which is not a multiple of the p of GF(p), there does indeed exist at least one g(x) in ring R which divides $x^n - 1$. It happens that this g(x) is irreducible with respect to GF(p). Recall that ring R [Chap 3 (a)] is just the set of polynomials which have coefficients in GF(p). When applied to GF(2), this says that for any odd integer n, an irreducible g(x) exists in R over GF(2) which divides $x^n - 1$. Our demonstration does not say precisely what the degree of that existent g(x) is, though it could be figured out. It is $\leq \varphi(n)$ as we shall see.

The degree of g(x) is n-k. It would perhaps be nice if one could find a g(x) having *any* desired degree less than the selected value of n, the code length. One might wonder whether for the special and practical case GF(2) this might even be possible. This would lead to an (n,k) cyclic code for any n and k < n.

Consider this little Maple program:

```
n := 8;
for N from 1 to 2^(n+1)-1 do   # go only as far as needed
 # compute polynomial for this value of N
  c := convert(N,base,2):
  p := sum(c[i]*x^(i-1),i=1..nops(c)):
# see if it has a remainder
  r := Rem(x^n-1,p,x) mod 2;
  if type(r,numeric) and r = 0 then print("N=",N,"degree=",nops(c)-1,"p(x)=",p, r) fi;
od:
```

You enter a value of n for $(x^n - 1)$ and it tries *all possible* polynomials in search of a g(x) that divides $x^n - 1$. These polynomials are generated by setting N = 1.2.3,,, and converting each integer N into binary and regarding that bit pattern as the coefficients of a polynomial in R over GF(2). Here is an encouraging sample run with n = 8 as shown:

$$n := 8$$

$$\text{"N="}, 1, \text{"degree="}, 0, \text{"p(x)="}, 1, 0$$

$$\text{"N="}, 3, \text{"degree="}, 1, \text{"p(x)="}, 1 + x, 0$$

$$\text{"N="}, 5, \text{"degree="}, 2, \text{"p(x)="}, 1 + x^2, 0$$

$$\text{"N="}, 15, \text{"degree="}, 3, \text{"p(x)="}, 1 + x + x^2 + x^3, 0$$

$$\text{"N="}, 17, \text{"degree="}, 4, \text{"p(x)="}, 1 + x^4, 0$$

$$\text{"N="}, 51, \text{"degree="}, 5, \text{"p(x)="}, 1 + x + x^4 + x^5, 0$$

$$\text{"N="}, 85, \text{"degree="}, 6, \text{"p(x)="}, 1 + x^2 + x^4 + x^6, 0$$

$$\text{"N="}, 255, \text{"degree="}, 7, \text{"p(x)="}, 1 + x + x^2 + x^3 + x^4 + x^5 + x^6 + x^7, 0$$

$$\text{"N="}, 257, \text{"degree="}, 8, \text{"p(x)="}, x^8 + 1, 0$$

For this value of n, we find a viable g(x) of every degree less than n. Viable just means we could create a cyclic code based on that g(x) (the case g(x) = 1 excluded).

Unfortunately, this is true for some values of n and not true for others. There is doubtless some theorem that explains which values of n work and which don't. Here are some values of n which are found not to have g(x) of every possible degree: n = 5,7,9,10,14,15. Some of these are prime, some not, some even, some odd. The run for n = 9 looks like this

$$n := 9$$

$$\text{"N=", 1, "degree=", 0, "p(x)=", 1, 0}$$

$$\text{"N=", 3, "degree=", 1, "p(x)=", } 1 + x, 0$$

$$\text{"N=", 7, "degree=", 2, "p(x)=", } 1 + x + x^2, 0$$

$$\text{"N=", 9, "degree=", 3, "p(x)=", } 1 + x^3, 0$$

$$\text{"N=", 73, "degree=", 6, "p(x)=", } 1 + x^3 + x^6, 0$$

$$\text{"N=", 219, "degree=", 7, "p(x)=", } 1 + x + x^3 + x^4 + x^6 + x^7, 0$$

$$\text{"N=", 511, "degree=", 8, "p(x)=", } 1 + x + x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^8, 0$$

$$\text{"N=", 513, "degree=", 9, "p(x)=", } x^9 + 1, 0$$

so that no g(x) exists of degree 4 or 5. The reason a degree is missing can be analyzed by writing the equation g(x)h(x) = x^n-1 where g and h are allowed arbitrary coefficients a,b,c.... For bad values of n, one is led to a set of equations for these coefficients which have no solution. For example, one might end up with the requirement that b + b + 1 = 0 and no b in GF(2) solves that equation.

With the above as introduction, we now start into a set of Facts, many of which are quite interesting in their own right. They lead to the final conclusion that some g(x) which divides x^n-1 does exist.

Fact 1: For any integer n not a multiple of prime p, one can find m such that n is a divisor of p^m - 1.

(E.1)

Proof: Saying that n is a divisor of p^m-1 is the same as saying Rem[(p^m-1)/n] = 0. This in turn is the same as saying Rem[p^m/n] = 1. If this is not obvious, it follows from Little Lemma 2 (1.31). Restating one more time, our theorem is equivalent to claiming there exists integer m such that p^m mod n = 1. Since we have assumed n is not a multiple of p, and that p is a prime number, we know that GCD(p,n) = 1, so p and n are coprime (relatively prime). After all, p cannot divide n, and nothing smaller than p can divide p but 1. A certain Euler's Theorem [see Refs Euler] claims that for any element of Mod(n) that is coprime to n (such as our p), there exists an integer k such that a^k mod n = 1. In our case, that says p^k mod n = 1. If we select m = k, then p^m mod n = 1 and therefore Rem[p^m/n] = 1 and therefore Rem[(p^m-1)/n] = 0 and therefore n is a divisor of p^m - 1 for this value of m. Our theorem merely claims that such an integer m exists. It happens, according to Euler's Theorem, that the integer m = k is none other than φ(n), Euler's totient function. Integer n can be larger than or smaller than p.

Verification: Here we check the above Fact for the first 20 prime numbers and all n < 1000:

```
primes := seq(ithprime(i),i=1..20);
```

$$primes := 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71$$

```
found := false:
for p in [primes] do
  for n from 1 to 1000 do
    if n mod p = 0 then next; fi;    #ignore n being multiple of p
    m := phi(n);
    r := p^m-1 mod n;
    if r <> 0 then found := true; print("exception found", p, m, n) ;fi;
  od;
od;
if found = false then print("no exceptions were found"); fi;
```

"no exceptions were found"

Fact 2: If integer D is a divisor of q -1, then GF(q) has at least one element of order D. (E.2)

Proof: We know from (4.21) that [order(α^k)] = (q-1)/GCD(k,q-1) where α is any primitive element of GF(q) and k any positive integer. Since D is a divisor of q-1 we can write DM = q-1 where M is the other factor. M then also divides q-1. Setting k = M,

[order(α^M)] = (q-1)/GCD(M,q-1) .

But GCD(M,q-1) = M. The reason is that M is a candidate GCD since it divides M and q-1, and no larger integer can divide M, so M is it. Thus we have shown that [order(α^M)] = (q-1)/M = D. Thus we have found an element of GF(q), namely α^M , which has order D, for any D among the divisors of (q-1).

Example: For GF(2^4) we have q-1 = 15 which has divisors 1,3,5 and 15. If α is a primitive element, then we know α^{15} = 1 since such an element has order q-1.

D	1	3	5	15
M	15	5	3	1
β^{order}=1	$(\alpha^{15})^1$= 1	$(\alpha^5)^3$= 1	$(\alpha^3)^5$= 1	$(\alpha^1)^{15}$= 1
order β	1	3	5	15

Here an element β of GF(q) has been found for each divisor of q-1. For D = 1, β = 1 and 1^1 = 1 so the identity always has an order to match D = 1. For D = 15 we just get the statement that α is a primitive element α^{15}= 1. It is the interior columns that are important.

Fact 3: If integer D is a divisor of q -1, then GF(q) has at least one minimum polynomial of period D. (E.3)

Proof: From the Fact 2, we know that GF(p^m) has at least one element (call it α) of order D. This element has a minimum polynomial m(x) of the form (x-α)(other factors) . From (5.66) we know that the period of

a minimum polynomial is the same as the order of the elements in its conjugate set (here including α), so since α has order D, there exists m(x) of period D. QED.

Example: Recall this enumeration (6.21) of the minimum polynomials of GF(2^4), where we have added the two trivial minimum polynomials shown in (5.24) which are always present :

$$
\begin{array}{lll}
p_1(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8) & = x^4 + x + 1 & 10011 \\
p_7(x) = (x-\alpha^7)(x-\alpha^{14})(x-\alpha^{13})(x-\alpha^{11}) & = x^4 + x^3 + 1 & 11001 \\
m_3(x) = (x-\alpha^3)(x-\alpha^6)(x-\alpha^{12})(x-\alpha^9) & = x^4 + x^3 + x^2 + x + 1 & 11111 \\
m_5(x) = (x-\alpha^5)(x-\alpha^{10}) & = x^2 + x + 1 & 111 \qquad (6.21) \\
m_0(x) = (x-\alpha^0) = (x-1); & & \\
m_{zero} = (x-0) = x; & &
\end{array}
$$

We shall now compute the period of each. First the polynomials are entered:

```
p1 := x^4+x+1:
p7 := x^4+x^3+1:
m3 := x^4+x^3+x^2+x+1:
m5 := x^2+x+1:
m0 := x-1:
mzero := x:
```

The following procedure scans n downward to find the period of polynomial f(x) :

```
period := proc(f,q,p) local per, n;
  per := infinity;
  for n from q by -1 to 1 do if Rem(x^n-1,f,x) mod p = 0 then per := n; fi; od;
  RETURN(per);
end:
```

And here are the resulting periods:

```
period(p1,15,2);
                        15
period(p7,15,2);
                        15
period(m3,15,2);
                         5
period(m5,15,2);
                         3
period(m0,15,2);
                         1
period(mzero,15,2);
                        ∞
```

As claimed in the Fact, there exists a minimum polynomial of period D for each D that divides p^m-1. The function x can never divide any x^n- 1 so the procedure sets period = ∞.

Fact 4: For any n not a multiple of p, there exists a g(x) which divides $x^n - 1$ and which can therefore be used to construct a cyclic code of length n. This g(x) is irreducible in GF(p). (E.4)

Proof: To find a suitable g(x) with coefficients in GF(p), we search through extension fields $GF(p^m)$ for m = 1,2,3 ... . We know from Fact 3 that, for any divisor D of $p^m - 1$, $GF(p^m)$ has a minimum polynomial m(x) of period D, so that m(x) divides x^D-1. If we can find a value of m such that $p^m - 1$ has a divisor D=n then m(x) divides $x^n - 1$ and this m(x) is a viable g(x). But Fact 1 says that we *can* find m such that n is a divisor of $p^m - 1$, namely, $m = \varphi(n)$. Thus, the field $GF(p^{\varphi(n)})$ has a suitable minimum polynomial that can be used for g(x).

Corollary: For any n not a multiple of p one can construct a cyclic code of length n whose polynomials have coefficients in GF(p). (E.5)

Reminder: It is likely that there are many viable g(x) that divide x^n-1 and there will be such viable g(x) even when n *is* a multiple of p as our examples with GF(2) earlier show (see n = 8 case). It just happens that the g(x) we find here in our existence proof happens to be a minimum polynomial of some Galois extension field GF(q) over GF(p). This g(x) is of course irreducible in GF(p), and may or may not be a primitive polynomial of GF(q).