Linear Cyclic Codes

This worksheet details the example of the linear cyclic code presented in the text.
The code has 128 code words hence it can encode the ASCII character set.
The code has hamming distance d(C) = 5 so it can correct up to 2 errors and detect up to 4 errors.
Michael Monagan, October 1998, October 2002, November 2007, November 2010.

```
> n := 2^4-1;
```

$$n := 15$$

The codes will be in $R = Z_2[x]/(x^n - 1)$.

```
> Factor( x^n-1 ) mod 2;
```

$$(x^4 + x^3 + 1)(x^4 + x + 1)(x^2 + x + 1)(x^4 + x^3 + x^2 + x + 1)(x + 1)$$

```
> g := Expand( (x^4+x^3+1)*(x^4+x^3+x^2+x+1) ) mod 2;
```

$$g := x^8 + x^4 + x^2 + x + 1$$

Construct the set Ig = { f(x) g(x) : f(x) in R } . Obviously we can't try all f(x) because there are too many : there are 2^{15} elements of R . But we know Ig should have $2^{(15-8)} = 128$ elements. Hence.

```
> Ig := {0,g}: f := 1:
  while nops(Ig) < 128 do
     f := Nextpoly(f,x) mod 2;
     Ig := Ig union { Rem(f*g,x^n-1,x) mod 2 };
  od:
```

Here is one of the elements of Ig.

```
> Ig[2];
```

$$x^8 + x^4 + x^2 + x + 1$$

```
> C := map( proc(a) local i; [seq(coeff(a,x,i),i=0..n-1)] end, Ig ):
> C[2];
```

$$[1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0]$$

```
> a := Ig[2];
```

$$a := x^8 + x^4 + x^2 + x + 1$$

```
> b := Ig[4];
```

$$b := x^9 + x^5 + x^3 + x^8 + x^4 + 1$$

```
> c := a-b mod 2;
```

$$x^9 + x^5 + x^3 + x^2 + x$$

A clever way to calculate the Hamming distance is

```
> subs( x=1, c );
```

$$5$$

So $d(I_2, I_4) = 5$ so the Hamming distance of this code is no more than 5.
Let's determine d(C). I'll print out a set of all the Hamming distances.

```
> d := proc(a,b) subs(x=1,a-b mod 2) end:
> { seq( d(c,0), c = Ig minus {0} ) };
```

$$\{5, 6, 7, 8, 9, 10, 15\}$$

So d(C) = 5 which means we have 2 bits of error correction and 4 for error detection.