TC10 / **4b. The Meggit decoder for cyclic codes**

S. Xambó

- Syndrome of the received vector (polynomial).
- The Meggitt table
- The Meggitt decoding algorithm

Syndromes

Let $g \in F[x]$ be the generating polynomial of a cyclic code C of length n over F. We want to implement the Meggitt decoder for C. In this decoder, a received vector $y = [y_0, \dots, y_{n-1}]$ is seen as a polynomial

$$y_0 + y_1 x + \cdots + y_{n-1} x^{n-1} \in F[x]_n$$

and by definition the *syndrome* of y, $S(y)$, is the remainder of the Euclidean division of y by g (in computational terms, `remainder(y,g)`). The vectors with zero syndrome are, again by definition, the vectors of C.

Proposition. We have the identity

$$S(xy) = S(xS(y)).$$

Proof. By definition of $S(y)$, there exists $q \in F[x]_n$ such that

$$y = qg + S(y).$$

Multiplying by x, and taking residue mod g, we get the result.

Corollary. If we set $S_0 = S(y)$ and

$$S_j = S(x^j y),\ j = 1, \ldots, n-1,$$

then $S_j = S(xS_{j-1})$.

The Meggitt table

If we want to correct t errors, where t is not greater than the error-correcting capacity, then the Meggitt decoding scheme presupposes the computation of a table E of the syndromes of the error-patterns of the form $ax^{n-1} + e$, where $a \in F^*$ and $e \in F[x]$ has degree $n-2$ (or less) and at most $t-1$ non-vanishing coefficients.

Example (Meggitt table of the binary Golay code). The binary Golay code can be defined as the length $n = 23$ cyclic code generated by

$$g = x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1 \in \mathbb{Z}_2[x]$$

and in this case, since the error-correcting capacity is 3, the Meggitt table can be encoded as follows:

```
# Meggitt table for the binary Golay code
n=23; R=0..(n-2);
g=x^11+x^9+x^7+x^6+x^5+x+1 : Zmod(2)[x];

# The table
E1=[remainder(x^(n-1),g) → x^(n-1)];
E2=[remainder(x^(n-1)+x^i,g) → x^(n-1)+x^i
         with i in R];
E3=[remainder(x^(n-1)+x^i+x^j,g) → x^(n-1)+x^i+x^j
    with (i,j) in (R,R) where j<i];
E=E1+E2+E3;

# Example
s=remainder(x^(n-1)+x^14+x^3,g) #
E(s) # → x^22+x^14+x^3
```

Thus we have that $E(s)$ is 0 for all syndromes s that do not coincide with the syndrome of x^{22}, or of $x^{22}+x^i$ for $i=0,\ldots,21$, or of $x^{22}+x^i+x^j$ for $i,j\in\{0,1,\ldots,21\}$ and $i>j$. Otherwise $E(s)$ selects, among those polynomials, the one that has syndrome s.

Example (Meggitt table of the ternary Golay code). The ternary Golay code can be defined as the length 11 cyclic code generated by

$$g = x^5 + x^4 + 2x^3 + x^2 + 2 \in \mathbb{Z}_3[x]$$

and in this case, since the error-correcting capacity is 2, the Meggitt table can be defined as follows:

```
# Meggitt table for the binary Golay code
n=11; R=0..(n-2);
U={1,-1};
g=x^5+x^4-x^3+x^2+1 : Zmod(3)[x];
# The table
E1=[remainder(u*x^(n-1),g) → u*x^(n-1)
        with u in U];
E2=[remainder(u*x^(n-1)+v*x^i,g)->u*x^(n-1)+v*x^i
        with (i,u,v) in (R,U,U)];
E=E1+E2;

# Example
s=remainder(-x^(n-1)+x^5,g) #
E(s) # → 2*x^10+x^5
```

The Meggitt algorithm

If y is the received vector (polynomial), the Meggitt algorithm goes as follows:

1) Find the syndrome $s = s_0$ of y.
2) If $s = 0$, return y (we know y is a code vector).
3) Otherwise compute, for $j = 1,2,\ldots,n-1$, the syndromes s_j of $x^j y$, and stop for the first $j \geq 0$ such that $e = E(s) \neq 0$.
4) Return $y - e/x^j$.

Remark. The s_j are computed recursively by $s_0 = s$ and $s_j = S(xs_{j-1})$.

Remark. The j in step 3 exists because the code is perfect.

```
# Meggitt decoder. We assume that g is known
meggitt(y):=
begin
  local x=variable(g), s=remainder(y,g), j=0, e
  if s==0 then say("Code vector "|y); return y end
  while E(s)==0 do
    j=j+1
    s=remainder(x*s,g)
  end
  e=E(s)/x^j; say("Error pattern; "|e)
  y=y-e
end;
```