III Codes cycliques

- Famille de codes linéaires avec distance garantie, faciles à construire et implémenter.
  - Cas particulier: codes de Reed-Solomon
- Très utilisés dans les applications pratiques

Codes cycliques

- **Rappel**: C code linéaire (n,k) == code engendré par une matrice G (k lignes, n colonnes) de rang k;
  les lignes de G sont formées par k mots de code linéairement indépendants.
- **Definition 1: Opérateur décalage** : $\sigma([c_0 \ldots, c_{n-1}]) = [c_{n-1}, c_0 \ldots, c_{n-2}]$
- **Définition 2** : Code cyclique $\Leftrightarrow$ code linéaire stable par σ
- Exemple: **code binaire cyclique (7,4) qui contient « 1011000 »**
- **Théorème 1: matrice génératrice d'un code cyclique**

  Un code cyclique (n,k) est équivalent à un code engendré par un mot de code $m=[c_0, \ldots, c_{n-k-1}, c_{n-k}=1, 0 \ldots, 0]$
- Intérêt 1: description simple, seulement r=n-k symboles de V

Caractérisation: polynôme générateur

- Tout mot $u \in V^n$ peut être représenté par un polynôme de degré n-1 :
  $u = [u_0, \ldots, u_{n-1}] \Leftrightarrow P_u = \Sigma_{i=0}^{n-1} u_i.X^i$
- **Lemme** : le mot $\sigma(c)$ est associé au polynôme :
  $P_{\sigma(C)} = X.P_c \bmod (X^n - 1)$
- **Définition 3**: **polynôme générateur** du code cyclique généré par le mot de code $m=[c_0, \ldots, c_{r-2}, c_{r-1}, c_r=1, 0 \ldots, 0]$
  $\mathbf{g(X) = P_m = \Sigma_{i=0}^{r-1} c_i.X^i + X^r}$
- **Théorème 2** : $\forall$ c mot de code, P_c est multiple de g(X)
- **Théorème 3** : g est un diviseur unitaire de $X^n - 1$de degré r

Codage/décodage code cyclique

- **Codage** : $P_{[a.G]} = g(X).P_a$
  - Tout mot de code est un multiple de g mod $X^n - 1$
  - Tout multiple de g mod $X^n - 1$ est un mot de code
- **Détection** : on reçoit $y = P_y$
  - Si P_y n'est pas multiple de g => erreur
  - Syndrome d'erreur: $P_e = P_y \bmod g$
- **Correction**: à partir du syndrome
  - (algorithme de Meggitt)
  - Si Poids (P_e) inférieur à (d-1)/2 : correction : $P_y - (P_y \bmod g)$
  - Cas général: algorithme de Berlekamp-Massey en O(n log n)

Distance minimale d'un code cyclique

- **Théorème 4 (dit BCH)** (n premier avec q)
  - Soit α racine primitive de $X^n - 1$ dans GF(q)
  - Si il existe a et b entiers tel que g(X) est multiple de $(X- \alpha^a) (X- \alpha^{a+1}) (X- \alpha^{a+2}) \dots (X- \alpha^{a+b-1})$

  Alors le code cyclique C de polynôme générateur g(X) est de distance : **$d(C) \geq b+1$**

  C est donc au moins [b/2]-correcteur (ou b-détecteur)

Codes binaires de Reed-Solomon

- **On choisit : $q = 2^m$** (donc V= {chiffres de m bits}) et **$n = 2^m - 1$**
- On a alors: $X^n - 1 = X^{q-1} - 1 = \prod_{a \in GF(q)^*} (X - a)$.
  - Si α générateur de GF(q)* : $\{ a \in GF(q)^* \} = \{\alpha^i / i=0..q-2\}$
    Donc $X^n - 1 = \prod_{a \in GF(q)^*} (X - \alpha^i)$
  - D'après BCH, il suffit de choisir $g = \prod_{i=a..a+r-1} (X - \alpha^i)$!!!
- **Définition 4** : code cyclique de Reed-Solomon RS(n, k) :
  RS(n,k) est un code cyclique de polynôme générateur
  $g(X) = \prod_{i=a..a+r-1} (X - \alpha^i)$ de degré r
- **Théorème 5** : RS(n,k) est de distance d = n-k+1 = r+1
  - D'après théorème BCH : $d \geq r+1$
  - D'après la borne de Singleton: $d \leq r+1$
- Ex. Galileo : RS(255,223) sur V={octets}, 16-correcteur
- NB RS(n,k) est de distance maximale sur GF(2^m) !!!
  … mais pas nécessairement parmi les codes binaires…