Ecole sur les Codes Correcteurs d'Erreurs" (Algérie)

Codes linéaires

Dr. Joël KABORE

Laboratoire de Mathématiques et Informatique (LAMI)
Université Joseph KI-ZERBO
Burkina-Faso

Septembre 2025

Objectifs

- Fondamentaux des codes linéaires sur anneaux
- Codes constacycliques sur les anneaux
- Applications de Gray

Base modulaire

Définition

Soit R un anneau fini. On dit que $\mathcal{C}(\subseteq R^n)$ est un code linéaire de longueur n si $\mathcal{C}$ est un R-sous module de R^n.

Base modulaire

Définition

Soit R un anneau fini. On dit que $\mathcal{C}(\subseteq R^n)$ est un code linéaire de longueur n si $\mathcal{C}$ est un R-sous module de R^n.

Soit R un anneau commutatif local fini, d'idéal maximal $\mathfrak{m}$.

- $v_1, ..., v_r \in R^n$ sont **modulairement indépendants** si $\forall\ (\alpha_1, ..., \alpha_r) \in R^r$

$$\sum_{i=1}^{r} \alpha_i v_i = 0 \Rightarrow \alpha_i \in \mathfrak{m},\ \forall\ i \in \{1, ..., r\}.$$

  - ▷ 0_{R^n} est modulairement dépendant.
  - ▷ $v \in R^n \setminus \{0\}$ est modulairement indépendant.

Base modulaire

Définition

Soit R un anneau fini. On dit que $\mathcal{C}(\subseteq R^n)$ est un code linéaire de longueur n si $\mathcal{C}$ est un R-sous module de R^n.

Soit R un anneau commutatif local fini, d'idéal maximal $\mathfrak{m}$.

- $v_1, ..., v_r \in R^n$ sont **modulairement indépendants** si $\forall\ (\alpha_1, ..., \alpha_r) \in R^r$

$$\sum_{i=1}^{r} \alpha_i v_i = 0 \Rightarrow \alpha_i \in \mathfrak{m},\ \forall\ i \in \{1, ..., r\}.$$

  - ▷ 0_{R^n} est modulairement dépendant.
  - ▷ $v \in R^n \setminus \{0\}$ est modulairement indépendant.
  - ▷ linéairement indépendants $\Rightarrow$ modulairement indépendants
  - ▷ modulairement indépendants $\not\Rightarrow$ linéairement indépendants.

Base modulaire

- Soient $\alpha_1, ...\alpha_r \in R$. On dit que des vecteurs non-nuls $v_1, ..., v_r \in R^n$ sont **indépendants** si

$$\sum_{i=1}^{r} \alpha_i v_i = 0 \Rightarrow \alpha_i v_i = 0, \ \forall \ i \in \{1, ..., r\}.$$

Base modulaire

- Soient $\alpha_1, ...\alpha_r \in R$. On dit que des vecteurs non-nuls $v_1, ..., v_r \in R^n$ sont **indépendants** si

$$\sum_{i=1}^{r} \alpha_i v_i = 0 \Rightarrow \alpha_i v_i = 0, \ \forall \ i \in \{1, ..., r\}.$$

  - ▷ vecteurs non-nuls indépendants $\Rightarrow$ modulairement indépendants
  - ▷ modulairement indépendants $\not\Rightarrow$ indépendants.

Matrice génératrice

- **Base modulaire** $\{v_1, ..., v_r\}$ de $\mathcal{C}$: indépendants, modulairement indépendants et engendrent E.

Matrice génératrice

- **Base modulaire** $\{v_1, ..., v_r\}$ de $\mathcal{C}$: indépendants, modulairement indépendants et engendrent E.
- La matrice G dont les lignes forment une base modulaire de $\mathcal{C}$ est appelée matrice génératrice de $\mathcal{C}$.

Matrice génératrice

Si R est un anneau à chaîne fini, tout code linéaire défini sur R admet une base modulaire et une matrice génératrice équivalente à la matrice G (dite sous forme standard)

$$G = \begin{pmatrix} I_{k_0} & A_{0,1} & A_{0,2} & A_{0,3} & \dots & A_{0,e-1} & A_{0,e} \\ 0 & \gamma I_{k_1} & \gamma A_{1,2} & \gamma A_{1,3} & \dots & \gamma A_{1,e-1} & \gamma A_{1,e} \\ 0 & 0 & \gamma^2 I_{k_2} & \gamma^2 A_{2,3} & \dots & \gamma^2 A_{2,e-1} & \gamma^2 A_{2,e} \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & \gamma^{e-1} I_{k_{e-1}} & \gamma^{e-1} A_{e-1,e} \end{pmatrix} \quad (1)$$

où I_k représente la matrice identité de taille k et $A_{i,j}$ sont des matrices de taille $k_i \times k_j$, avec $0 \leq i \leq e-1$ et $1 \leq j \leq e$.

Matrice génératrice

$\mathcal{C}$ code linéaire de longeur n de matrice génératrice G sous forme standard.

- $\mathcal{C}$ est de type $(k_0, k_1, \cdots, k_{e-1})$.
- $|\mathcal{C}| = |K|^{\sum_{i=0}^{e-1}(e-i)k_i}$.
- Rang de $\mathcal{C} = \sum_{i=0}^{e-1} k_i$.
- $\mathcal{C}$ est un code libre si Rang de $\mathcal{C} = k_0$

Dual

On munit le module R^n de la forme bilinéaire symétrique standard "." : $R^n \times R^n \longrightarrow R$ définie par :

$$a.b = \sum_{i=1}^{n} a_i b_i;\ \forall\ a = (a_1, ..., a_n), b = (b_1, ..., b_n) \in R^n.$$

- Code dual : $\mathcal{C}^{\perp} = \{a \in R^n : a.b = 0, \forall\ b \in \mathcal{C}\}$.
- Si $\mathcal{C} \subset \mathcal{C}^{\perp}$, on dit que le code est auto-orthogonal et si $\mathcal{C} = \mathcal{C}^{\perp}$, on dit qu'il est auto-dual.
- $(\mathcal{C}^{\perp})^{\perp} = \mathcal{C}$

Dual

Si la matrice génératrice de $\mathcal{C}$ sous forme stantard G alors matrice de contrôle de $\mathcal{C}$:

$$H = \begin{pmatrix} B_{0,e} & B_{0,e-1} & \dots & B_{0,1} & I_{n-k} \\ \gamma B_{1,e} & \gamma B_{1,e-1} & \dots & \gamma I_{k_{e-1}} & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ \gamma^{e-1} B_{e-1,e} & \gamma^{e-1} I_{k_1} & \dots & 0 & 0 \end{pmatrix}$$

où $B_{i,j} = -\sum_{k=i+1}^{j-1} B_{i,k} A^t_{e-j,e-k} - A^t_{e-j,e-i}$, $\forall\ 0 \leq i < j \leq e$.

Dual

Si la matrice génératrice de $\mathcal{C}$ sous forme stantard G alors matrice de contrôle de $\mathcal{C}$:

$$H = \begin{pmatrix} B_{0,e} & B_{0,e-1} & \cdots & B_{0,1} & I_{n-k} \\ \gamma B_{1,e} & \gamma B_{1,e-1} & \cdots & \gamma I_{k_{e-1}} & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ \gamma^{e-1} B_{e-1,e} & \gamma^{e-1} I_{k_1} & \cdots & 0 & 0 \end{pmatrix}$$

où $B_{i,j} = -\sum_{k=i+1}^{j-1} B_{i,k} A^t_{e-j,e-k} - A^t_{e-j,e-i}$, $\forall\ 0 \leq i < j \leq e$.

▷ $|\mathcal{C}||\mathcal{C}^{\perp}| = |R|^n$.

Identité de MacWilliams

- Polynôme enumerateur de Poids :
  $W_{\mathcal{C}}(X, Y) = \sum_{c \in \mathcal{C}} X^{n-w(c)} Y^{w(c)} = \sum_{i=0}^{n} A_i X^{n-i} Y^i$, où A_i est le nombre de mots de poids i.
  La série $(A_0, ..., A_n)$ est appelée distribution des poids des mots du code $\mathcal{C}$.

Identité de MacWilliams

- Polynôme enumerateur de Poids :
  $W_{\mathcal{C}}(X,Y) = \sum_{c\in\mathcal{C}} X^{n-w(c)}Y^{w(c)} = \sum_{i=0}^{n} A_i X^{n-i}Y^i$, où A_i est le nombre de mots de poids i.
  La série $(A_0, ..., A_n)$ est appelée distribution des poids des mots du code $\mathcal{C}$.
- Si $W_{\mathcal{C}}(X,Y)$ est l'énumérateur de poids du code $\mathcal{C}$, alors :

$$W_{\mathcal{C}^\perp}(X,Y) = \frac{1}{|\mathcal{C}|} W_{\mathcal{C}}(X + (|R|-1)Y, X - Y).$$

Codes constacycliques

Soient $\lambda \in U(R)$ et σ_λ le λ-shift défini par :

$$\begin{array}{rccc} \sigma_\lambda : & R^n & \longrightarrow & R^n \\ & (a_0, ..., a_{n-1}) & \longmapsto & (\lambda a_{n-1}, ..., a_{n-2}) \end{array}$$

- Un code linéaire $\mathcal{C}$ de longueur n sur R est dit λ-constacyclique si $\sigma_\lambda(\mathcal{C}) \subseteq \mathcal{C}$.

Soit φ l'application qui à tout vecteur $a = (a_0, a_1, ..., a_{n-1})$ de R^n associe l'élément dans $\frac{R[X]}{<X^n-\lambda>} = R[x]$, défini par $a(x) = a_0 + a_1 x + ... + a_{n-1}x^{n-1}$ où $x = X + < X^n - \lambda >$ est la classe de X dans $\frac{R[X]}{<X^n-\lambda>}$.

- $\sigma_\lambda(a) \rightleftharpoons xa(x)$

Soit φ l'application qui à tout vecteur $a = (a_0, a_1, ..., a_{n-1})$ de R^n associe l'élément dans $\frac{R[X]}{<X^n-\lambda>} = R[x]$, défini par $a(x) = a_0 + a_1x + ... + a_{n-1}x^{n-1}$ où $x = X + < X^n - \lambda >$ est la classe de X dans $\frac{R[X]}{<X^n-\lambda>}$.

- $\sigma_\lambda(a) \rightleftharpoons xa(x)$
- $\mathcal{C}$ est un code λ- constacyclique de longueur $n \Leftrightarrow \varphi(\mathcal{C})$ est un idéal de $\frac{R[X]}{<X^n-\lambda>}$.

Soit φ l'application qui à tout vecteur $a = (a_0, a_1, ..., a_{n-1})$ de R^n associe l'élément dans $\frac{R[X]}{<X^n-\lambda>} = R[x]$, défini par $a(x) = a_0 + a_1x + ... + a_{n-1}x^{n-1}$ où $x = X + < X^n - \lambda >$ est la classe de X dans $\frac{R[X]}{<X^n-\lambda>}$.

- $\sigma_\lambda(a) \rightleftharpoons xa(x)$
- $\mathcal{C}$ est un code λ- constacyclique de longueur $n \Leftrightarrow \varphi(\mathcal{C})$ est un idéal de $\frac{R[X]}{<X^n-\lambda>}$.
- $\mathcal{C}^\perp$ est un code λ^{-1}- constacyclique.

dual

Proposition

Soient R un anneau fini et λ un élément inversible de R.
Alors $a(x)b(x) = 0$ dans $R[x](= \frac{R[X]}{<X^n-\lambda>}) \Leftrightarrow (a_0, a_1, ..., a_{n-1})$ est orthogonal à $(b_{n-1}, b_{n-2}, ..., b_0)$ et à tous les décalages λ^{-1}-constacyclique de b.

Preuve :

- Pour tout $l = 0, 1, ..., m$ et $j = 0, 1, ..., n$, on a :

$$\sigma^j(a_{n-1}, a_{n-2}, ..., a_0) = \lambda^l \sigma^{ln+j}(a_{n-1}, ..., a_0).$$

dual

Proposition

Soient R un anneau fini et λ un élément inversible de R.
Alors $a(x)b(x) = 0$ dans $R[x](= \frac{R[X]}{<X^n-\lambda>}) \Leftrightarrow (a_0, a_1, ..., a_{n-1})$ est orthogonal à $(b_{n-1}, b_{n-2}, ..., b_0)$ et à tous les décalages λ^{-1}-constacyclique de b.

Preuve :

- Pour tout $l = 0, 1, ..., m$ et $j = 0, 1, ..., n$, on a :

$$\sigma^j(a_{n-1}, a_{n-2}, ..., a_0) = \lambda^l \sigma^{ln+j}(a_{n-1}, ..., a_0).$$

- $c(x) = a(x)b(x) = c_0 + c_1x + ... + c_{n-1}x^{n-1} \in R[x]$.
  $c_k =$
  $(a_0b_k + a_1b_{k-1} + ... + a_kb_0) + \lambda(a_{k+1}b_{n-1} + a_{k+2}b_{n-2} + ... + a_{n-1}b_{k+1})$
  $= \lambda(a_0, a_1, ..., a_{n-1}).\sigma^{k+1}(b_{n-1}, b_{n-2}, ..., b_0).$

dual

Proposition

Soient R un anneau fini et λ un élément inversible de R.
Alors $a(x)b(x) = 0$ dans $R[x](= \frac{R[X]}{<X^n-\lambda>}) \Leftrightarrow (a_0, a_1, ..., a_{n-1})$ est orthogonal à $(b_{n-1}, b_{n-2}, ..., b_0)$ et à tous les décalages λ^{-1}-constacyclique de b.

Preuve :

- Pour tout $l = 0, 1, ..., m$ et $j = 0, 1, ..., n$, on a :

$$\sigma^j(a_{n-1}, a_{n-2}, ..., a_0) = \lambda^l \sigma^{ln+j}(a_{n-1}, ..., a_0).$$

- $c(x) = a(x)b(x) = c_0 + c_1x + ... + c_{n-1}x^{n-1} \in R[x]$.
  $c_k =$
  $(a_0b_k + a_1b_{k-1} + ... + a_kb_0) + \lambda(a_{k+1}b_{n-1} + a_{k+2}b_{n-2} + ... + a_{n-1}b_{k+1})$
  $= \lambda(a_0, a_1, ..., a_{n-1}).\sigma^{k+1}(b_{n-1}, b_{n-2}, ..., b_0)$.
- $c(x) = 0 \Leftrightarrow (a_0, a_1, ..., a_{n-1}).\sigma^{k+1}(b_{n-1}, b_{n-2}, ..., b_0) = 0$ pour $k = 0, 1, ..., n-1$

Dual

Soient I un idéal de $R[X]$ et $I^* = \{f^*(x) \in R[x] : f(x) \in I\}$. Soit $f(X) = a_0 + a_1X + ... + a_rX^r$ un polynôme de degré r dans $R[X]$ et i le plus petit indice tel que $a_i \neq 0$.

- Le polynôme réciproque de f :
  $f^* = X^{r+i}f(\frac{1}{X}) = a_rX^i + a_{r-1}X^{i+1} + a_{r-2}X^{i+2} + ... + a_iX^r$.
- Annulateur de I : idéal
  $\mathcal{A}(I) = \{g(x) \in R[x] : f(x)g(x) = 0, \forall f(x) \in I\}$.

Dual

Soient I un idéal de $R[X]$ et $I^* = \{f^*(x) \in R[x] : f(x) \in I\}$. Soit $f(X) = a_0 + a_1X + ... + a_rX^r$ un polynôme de degré r dans $R[X]$ et i le plus petit indice tel que $a_i \neq 0$.

- Le polynôme réciproque de f :
  $f^* = X^{r+i}f(\frac{1}{X}) = a_rX^i + a_{r-1}X^{i+1} + a_{r-2}X^{i+2} + ... + a_iX^r$.
- Annulateur de I : idéal
  $\mathcal{A}(I) = \{g(x) \in R[x] : f(x)g(x) = 0, \forall f(x) \in I\}$.

Proposition

Soit $\mathcal{C}$ un code λ-constacyclique de longueur n sur R.

$$\mathcal{C}^\perp = \mathcal{A}(\mathcal{C})^*$$

Dual

Soient I un idéal de $R[X]$ et $I^* = \{f^*(x) \in R[x] : f(x) \in I\}$. Soit $f(X) = a_0 + a_1X + ... + a_rX^r$ un polynôme de degré r dans $R[X]$ et i le plus petit indice tel que $a_i \neq 0$.

- Le polynôme réciproque de f :
  $f^* = X^{r+i}f(\frac{1}{X}) = a_rX^i + a_{r-1}X^{i+1} + a_{r-2}X^{i+2} + ... + a_iX^r$.
- Annulateur de I : idéal
  $\mathcal{A}(I) = \{g(x) \in R[x] : f(x)g(x) = 0, \forall f(x) \in I\}$.

Proposition

Soit $\mathcal{C}$ un code λ-constacyclique de longueur n sur R.

$$\mathcal{C}^\perp = \mathcal{A}(\mathcal{C})^*$$

Preuve :

- $\mathcal{C}^{\perp}$ est un code λ^{-1}-constacyclique
- Soit $b = (b_0, ..., b_{n-1}) \in \mathcal{C}^{\perp}$, $a = (a_0, ..., a_{n-1}) \in \mathcal{C}$ alors $a(x)b^*(x) = 0$ dans $R[x]$; d'où $\mathcal{C}^{\perp} \subseteq \mathcal{A}(\mathcal{C})^*$.

Preuve :

- $\mathcal{C}^{\perp}$ est un code λ^{-1}-constacyclique
- Soit $b = (b_0, ..., b_{n-1}) \in \mathcal{C}^{\perp}$, $a = (a_0, ..., a_{n-1}) \in \mathcal{C}$ alors $a(x)b^*(x) = 0$ dans $R[x]$; d'où $\mathcal{C}^{\perp} \subseteq \mathcal{A}(\mathcal{C})^*$.

Preuve :

- $\mathcal{C}^{\perp}$ est un code λ^{-1}-constacyclique
- Soit $b = (b_0, ..., b_{n-1}) \in \mathcal{C}^{\perp}$, $a = (a_0, ..., a_{n-1}) \in \mathcal{C}$ alors $a(x)b^*(x) = 0$ dans $R[x]$; d'où $\mathcal{C}^{\perp} \subseteq \mathcal{A}(\mathcal{C})^*$.
- Réciproquement, $b(x) = b_0 + b_1x + ... + b_{n-1}x^{n-1} \in \mathcal{A}(\mathcal{C})^* \Rightarrow b^*(x) \in \mathcal{A}(\mathcal{C}) \Rightarrow a(x)b^*(x) = 0, \ \forall \ a(x) \in \mathcal{C}$; d'où $\mathcal{A}(\mathcal{C})^* \subseteq \mathcal{C}^{\perp}$.

Exemple Soit $\mathcal{C}$ le code linéaire de longueur 4 défini sur $\mathbb{Z}_4$ par :

$$\begin{aligned}\mathcal{C} = \quad & \{0000, 1113, 2222, 3331, 0202, 1311, 2020, 3133, \\ & 0022, 1131, 2200, 3313, 0220, 1333, 2002, 3111.\}\end{aligned}$$

"Gray map"

Soit R un anneau et R_0 un sous anneau de R.

- Application de Gray : $\phi : R \to R_0^t$, t un entier et conserve les distances.

"Gray map"

Soit R un anneau et R_0 un sous anneau de R.

- Application de Gray : $\phi : R \to R_0^t$, t un entier et conserve les distances.
- En général les distances R_0^t muni de la distance de Hamming d_H et R munit d'une distance d tel que $d(r_1, r_2) = d_H(\phi(r_1), \phi(r_2)$.
- Une application de Gray peut être linéaire ou pas.
- $\phi(\mathcal{C})$ peut être un code linéaire ou pas.

"Gray map" sur $\mathbb{Z}_4$

Proposition

Soit $\mathcal{C}$ un code linéaire de longueur n sur $\mathbb{Z}_4$. Alors $\phi(\mathcal{C})$ est un code linéaire si et seulement si

$$u, v \in \mathcal{C} \Rightarrow 2\overline{u}.\overline{v} \in \mathcal{C}.$$

où $\overline{u} = u + 2\mathbb{Z}$ et $\overline{u}.\overline{v} = \sum_i^n u_i v_i$.
Dans ce cas si $\mathcal{C} =< L_1, L_2, \cdots, L_t >$, alors
$\phi(\mathcal{C}) =< \phi(L_1), \phi(-L_1), \phi(L_2), \phi(-L_1) \cdots, \phi(L_t) >, \phi(-L_t) >$

"Gray map" sur $\mathbb{Z}_4$

Proposition

Soit $\mathcal{C}$ un code linéaire de longueur n sur $\mathbb{Z}_4$. Alors $\phi(\mathcal{C})$ est un code linéaire si et seulement si

$$u, v \in \mathcal{C} \Rightarrow 2\overline{u}.\overline{v} \in \mathcal{C}.$$

où $\overline{u} = u + 2\mathbb{Z}$ et $\overline{u}.\overline{v} = \sum_i^n u_i v_i$.
Dans ce cas si $\mathcal{C} =< L_1, L_2, \cdots, L_t >$, alors
$\phi(\mathcal{C}) =< \phi(L_1), \phi(-L_1), \phi(L_2), \phi(-L_1) \cdots, \phi(L_t) >, \phi(-L_t) >$

- $r \in \mathbb{Z}_4 \Rightarrow r = a + 2b;\ a, b \in \mathbb{F}_2$
- $$\begin{array}{rccc} \phi: & \mathbb{Z}_4 & \longrightarrow & \mathbb{F}_2^2 \\ & r = a + 2b & \longmapsto & (b, a + b) \end{array}$$
- ϕ n'est pas linéaire

- $$\begin{array}{rccc} \phi: & (\mathbb{Z}_4^n, d) & \longrightarrow & (\mathbb{F}_2^{2n}, d_H) \\ & (r_1, r_2, \cdots, r_n) & \longmapsto & (\phi(r_1), \phi(r_2), \cdots, \phi(r_n)) \end{array}$$

- $$\begin{array}{rccc} \phi: & (\mathbb{Z}_4^n, d) & \longrightarrow & (\mathbb{F}_2^{2n}, d_H) \\ & (r_1, r_2, \cdots, r_n) & \longmapsto & (\phi(r_1), \phi(r_2), \cdots, \phi(r_n)) \end{array}$$
- $d_L(r, 0) = W_L(r) = W_H(\phi(r)) \Rightarrow W_L(r) := \begin{cases} 0, & r = 0 \\ 2, & r = 2 \\ 1, & r \in \{1; 3\} \end{cases}$
- $W_L(r_1, r_2, \cdots, r_n) = \sum_{i=1}^{n} W_L(r_i)$.

- $$\begin{array}{rccc} \phi: & (\mathbb{Z}_4^n, d) & \longrightarrow & (\mathbb{F}_2^{2n}, d_H) \\ & (r_1, r_2, \cdots, r_n) & \longmapsto & (\phi(r_1), \phi(r_2), \cdots, \phi(r_n)) \end{array}$$
- $d_L(r, 0) = W_L(r) = W_H(\phi(r)) \Rightarrow W_L(r) := \begin{cases} 0, & r = 0 \\ 2, & r = 2 \\ 1, & r \in \{1; 3\} \end{cases}$
- $W_L(r_1, r_2, \cdots, r_n) = \sum_{i=1}^{n} W_L(r_i)$.
  ▷ Poids de Lee et distance de Lee $d_L(r, s) = W_L(r - s)$.
  ▷ $\phi : (\mathbb{Z}_4^n, d) \longrightarrow (\mathbb{F}_2^{2n}, d_H)$ est une isométrie.

La classe des anneaux finis de Frobenius est la plus grand classe d'anneaux finis dans laquelle l'identité de MacWilliams reste valable.

- Steven T. Dougherty, *Algebraic Coding Theory Over Finite Commutative Rings*, SpringerBriefs in Mathematics, New-York, 2017.
- Huffman, W. C. AND Pless, V. , *Fundamentals of Error-Correcting Codes*, Cambridge University Press, New-York, 2003.
- MacWilliams, F.J. AND Sloane, N.J.A. *The Theory of Error-Correcting Codes*, Bell Laboratories Murray Hill NJ 07974 U.S.A, 1981.