IV.5.b. Montrer que :

$$\begin{cases} u_r = f_1 + K\sin\theta + G\cos\theta \\ u_\theta = f_2 + K\cos\theta - G\sin\theta + Hr \end{cases}$$

où f_1 et f_2 sont des fonctions de $A, B, D, A', B', C', \nu, E, r, \theta$ que l'on précisera et K, G, H sont des constantes réelles. A quoi correspondent les termes en K, G, H ?

PROBABILITÉS ET STATISTIQUES

Notations et Définitions

On se donne un espace probabilisé $(\Omega, \mathcal{A}, \mathbb{P})$, c'est à dire un ensemble Ω muni d'une tribu $\mathcal{A}$ et d'une loi de probabilité $\mathbb{P}$. Pour abréger, on appellera *v.a.r. sur* $(\Omega, \mathcal{A})$ toute variable aléatoire réelle sur $(\Omega, \mathcal{A})$, et *v.a. sur* $(\Omega, \mathcal{A})$ *à valeurs dans* $(X, \mathcal{B})$ toute application mesurable de $(\Omega, \mathcal{A})$ dans $(X, \mathcal{B})$, lorsque X est un ensemble muni d'une tribu $\mathcal{B}$.

• Pour une v.a.r. Z sur $(\Omega, \mathcal{A})$, on pose $\mathbb{E}(Z) = \int_\Omega Z(\omega)\mathbb{P}(d\omega)$, si Z est positive ou intégrable, et $\|Z\|_r = (\mathbb{E}(|Z|^r))^{1/r}$ pour tout nombre réel $r \geq 1$.

• On appelle *variable de Bernoulli symétrique* toute v.a.r. Y sur $(\Omega, \mathcal{A})$ telle que $\mathbb{P}(Y = 1) = \mathbb{P}(Y = -1) = 1/2$.

• Soient $V, T \subset X$ et x un point de X. On pose alors:
$V \setminus T = \{s \in V \mid s \notin T\}$ et $V \triangle T = (V \setminus T) \cup (T \setminus V)$,
$\mathbb{1}_V(x) = 1$ si $x \in V$, et $\mathbb{1}_V(x) = 0$ sinon,
$\#(V) =$ cardinal(V) si V est fini, et $\#(V) = +\infty$ sinon.

• Pour chaque $x = (x_1, \cdots, x_n) \in X^n$, on considère sur $(X, \mathcal{B})$ la loi de probabilité $\nu_n^x : A \in \mathcal{B} \longmapsto \frac{1}{n}(\mathbb{1}_A(x_1) + \cdots + \mathbb{1}_A(x_n))$ (*loi empirique sur* $(x_1, \cdots, x_n)$).

• On rappelle le résultat suivant sur les v.a. indépendantes (c'est simplement une forme du *théorème de Fubini*):
soient Y et Z des v.a. indépendantes sur $(\Omega, \mathcal{A})$ à valeurs respectivement dans $(B, \mathcal{B})$ et $(C, \mathcal{C})$; soit f une application mesurable de $(B \times C, \mathcal{B} \otimes \mathcal{C})$ dans $[0, +\infty]$;
alors l'application $g : y \longmapsto \mathbb{E}(f(y, Z))$ est mesurable
et on a $\mathbb{E}(f(Y, Z)) = \mathbb{E}(g(Y))$.

• On appellera par abus de language *distance* sur un ensemble U toute application $d : U^2 \longrightarrow [0, +\infty[$ vérifiant $d(u, u) = 0$, $d(u, v) = d(v, u)$ et $d(u, w) \leq d(u, v) + d(v, w)$ pour tous $u, v, w \in U$ ($d(u, v) = 0$ n'implique pas nécessairement $u = v$).
Si U est un ensemble muni d'une distance d, on pose $\text{diam}(U) = \sup_{u,v \in U} d(u, v)$; on dit qu'une partie T de U est *ε-discernable* si on a $d(s, t) > \varepsilon$ pour tous s, t distincts dans T; on dit que T est *ε-dense* dans U si, pour chaque $u \in U$, il existe $u_T \in T$ avec $d(u, u_T) \leq \varepsilon$; on dit que T est un *ε-réseau* de U si T est à la fois ε-discernable et ε-dense dans U.
Lorsque U est fini, on admettra l'existence d'ε-réseaux pour chaque $\varepsilon \in]0, +\infty[$ quelle que soit d (un ε-réseau s'obtient en choisissant successivement des points de U de distances mutuelles $> \varepsilon$; au bout d'un nombre fini de choix, on doit s'arrêter).

• Si Q est une loi de probabilité sur $(X, \mathcal{B})$, on pose $d_Q(V,T) = Q(V \triangle T)$ pour tous $V, T \in \mathcal{B}$.

Les parties I et II sont indépendantes. La partie III dépend des parties I et II. La partie IV fournit des exemples d'application de la partie III.

Question préliminaire.
Soit Q une loi de probabilité sur $(X, \mathcal{B})$; montrer que $d_Q : (V,T) \longmapsto Q(V \triangle T)$ est une distance sur $\mathcal{B}$.

Première Partie

On fixe un entier $n > 0$.

Soient $Y_1, \cdots, Y_n$ des variables de Bernoulli symétriques indépendantes sur $(\Omega, \mathcal{A})$. Pour chaque $a = (a_1, \cdots, a_n) \in \mathbb{R}^n$, on considère la v.a.r. $Z(a) : \omega \longmapsto |\sum_{i=1}^n a_i Y_i(\omega)|$.
Pour tous $p_1, \cdots, p_n$ entiers ≥ 0 de somme p, on pose

$$c(p; p_1, \cdots, p_n) = \frac{p!}{p_1! \cdots p_n!}.$$

On rappelle la *formule multinomiale*:

$$(\sum_{i=1}^n a_i)^p = \sum_{p_1, \cdots, p_n} c(p; p_1, \cdots, p_n) a_1^{p_1} \cdots a_n^{p_n}$$

où la somme est prise sur tous les $p_1, \cdots, p_n$ entiers ≥ 0 de somme p.

On se propose de montrer que $\|Z(a)\|_r$ et $\|Z(a)\|_2$ sont comparables pour tout $r \in [1, +\infty[$ indépendamment de a et de n.

1.
(a) Soient $p_1, \cdots, p_n$ des entiers ≥ 0. Montrer que $\mathbb{E}(\prod_{i=1}^n Y_i^{p_i})$ est nul dès que l'un des p_i est impair.
(b) Montrer que $\mathbb{E}(Z(a)^2)$ vaut $\sum_{i=1}^n a_i^2$.
(c) Soit p un entier ≥ 0. Montrer que $\mathbb{E}(Z(a)^{2p})$ vaut

$$\sum_{p_1, \cdots, p_n} c(2p; 2p_1, \cdots, 2p_n) a_1^{2p_1} \cdots a_n^{2p_n},$$

où la somme est prise sur tous les $p_1, \cdots, p_n$ entiers ≥ 0 de somme p.

2. Montrer que $c(2p; 2p_1, \cdots, 2p_n)$ est majoré par $\frac{(2p)!}{p!} c(p; p_1, \cdots, p_n)$ pour tout entier $p \geq 0$ et tous $p_1, \cdots, p_n$ entiers ≥ 0 de somme p.
En déduire l'inégalité suivante, pour tout entier $p \geq 0$:

$$\mathbb{E}(Z(a)^{2p}) \leq \frac{(2p)!}{p!} (\mathbb{E}(Z(a)^2))^p.$$

3. Montrer que $\|Z(a)\|_r$ est majoré par $\sqrt{r}\, \|Z(a)\|_2$ pour tout $a \in \mathbb{R}^n$ et tout entier pair $r \geq 2$. En déduire l'encadrement suivant:

$$\|Z(a)\|_2 \leq \|Z(a)\|_t \leq \sqrt{t+2}\, \|Z(a)\|_2$$

pour tout $a \in \mathbb{R}^n$ et tout nombre réel $t \geq 2$.

4. Soient s, t des nombres réels positifs ($1 \leq s \leq 2 \leq t < +\infty$); on définit λ par $\frac{1}{2} = \lambda\frac{1}{s} + (1-\lambda)\frac{1}{t}$.
Montrer que, pour toute v.a.r. X sur $(\Omega, \mathcal{A})$, $\|X\|_2$ est majoré par $\|X\|_s^{\lambda}\|X\|_t^{1-\lambda}$.
En déduire l'encadrement suivant:

$$\|Z(a)\|_s \leq \|Z(a)\|_2 \leq 2^{\frac{4-2s}{s}}\|Z(a)\|_s.$$

pour tout $a \in \mathbb{R}^n$ et tout nombre réel $s \in [1,2]$.

5. Montrer que $(2p)!$ est majoré par $4^p(p!)^2$. En déduire l'inégalité suivante:

$$\mathbb{E}(\exp(\lambda Z(a)^2/\|Z(a)\|_2^2)) \leq \frac{1}{1-4\lambda}$$

pour tout $a \in \mathbb{R}^n$ et tout nombre réel λ de module $< 1/4$.

6. Soit r un nombre réel > 2. Si $(\Omega, \mathcal{A}, \mathbb{P})$ est le segment $[0,1]$ muni de la tribu borélienne et de la mesure de Lebesgue, indiquer quel est l'ensemble des valeurs que peut prendre $\|X\|_r/\|X\|_2$ quand X décrit l'ensemble des v.a.r. de carré intégrable sur $(\Omega, \mathcal{A})$.

Seconde Partie

Soit U un ensemble et soit $(Z_u)_{u\in U}$ une famille de v.a.r. sur $(\Omega, \mathcal{A})$. On fixe $r \in [1, +\infty[$ et on munit U de la distance $d_{(r)} : (u,v) \mapsto \|Z_u - Z_v\|_r$.
On suppose que $\mathrm{diam}(U)$ est fini et vaut δ.

On pose $\varepsilon_i = \delta 2^{-i}$ pour tout i entier ≥ 0.
Dans les questions 1, 2 et 3, on suppose que U est fini et on note ℓ le plus petit entier i tel que l'on ait $d(u,v) > \varepsilon_i$ pour tous $u, v \in U$ distincts.
Dans les questions 4 et 5, on suppose que U est dénombrable.

Soient $c \geq 0$ et $\beta \geq 0$. On suppose que toute partie ε-discernable de U (lorsque U est muni de la distance $d_{(r)}$) est de cardinal inférieur ou égal à $c\varepsilon^{-\beta}$, quel que soit $\varepsilon \in]0, \delta]$.
On se propose d'évaluer $\|\sup_{u\in U}|Z_u|\|_r$ sous cette hypothèse.

1. Etablir l'encadrement suivant:

$$\sup_{u\in U}\mathbb{E}(|Z_u|^r) \leq \mathbb{E}(\sup_{u\in U}|Z_u|^r) \leq \#(U)\sup_{u\in U}\mathbb{E}(|Z_u|^r).$$

2. Fixons $s \in U$; on se donne $T_0 = \{s\}$, $T_\ell = U$ et, pour chaque $i = 1, \cdots, \ell-1$, un ε_i-réseau T_i de U. Montrer que T_0 est un ε_0-réseau et que T_ℓ est un ε_ℓ-réseau et que chaque T_i (pour $i = 0, \cdots, \ell$) est de cardinal inférieur ou égal à $c\varepsilon_i^{-\beta}$.
Montrer que, pour chaque $i = 0, \cdots, \ell-1$, on peut trouver une application π_i : $T_{i+1} \longrightarrow T_i$ avec $d_{(r)}(s, \pi_i(s)) \leq \varepsilon_i$ pour tout $s \in T_{i+1}$.

3. Pour chaque $i = 0, \cdots, \ell$, on pose $W_i = \sup_{s\in T_i}|Z_s|$; montrer que, pour chaque $i = 0, \cdots, \ell-1$, $\|W_{i+1}\|_r$ est majoré par $\|W_i\|_r + \varepsilon_i\,(\#(T_{i+1}))^{1/r}$ (on pourra utiliser la question II.1). En déduire l'inégalité suivante:

$$\|\sup_{u\in U}|Z_u|\|_r \leq \|Z_s\|_r + \sum_{i=0}^{\ell-1}\varepsilon_i\,(\#(T_{i+1}))^{1/r}.$$

4. On suppose désormais que U est dénombrable, et non plus fini, et on fixe $s \in U$. Etablir l'inégalité suivante:

$$\| \sup_{u \in U} |Z_u| \|_r \leq \|Z_s\|_r + \sum_{i=0}^{\infty} \varepsilon_i \, c^{1/r} \, \varepsilon_{i+1}^{-\beta/r}.$$

5. Montrer que, dès que $r > 2\beta$,

$$\| \sup_{u \in U} |Z_u| \|_r \text{ est majoré par } \|Z_s\|_r + 5c^{1/r} \, \delta^{1-(\beta/r)}.$$

Troisième Partie

Soit X un ensemble muni de la tribu $\mathcal{B}$ et soient $X_1, \cdots, X_n, X'_1, \cdots, X'_n$ des v.a. sur $(\Omega, \mathcal{A})$ à valeurs dans $(X, \mathcal{B})$, indépendantes et de loi P; soient $Y_1, \cdots, Y_n$ des variables de Bernoulli symétriques sur $(\Omega, \mathcal{A})$ indépendantes entre elles et indépendantes de la suite $(X_1, \cdots, X_n, X'_1, \cdots, X'_n)$.
Soit $x = (x_1, \cdots, x_n) \in X^n$; on pose alors pour tout $B \in \mathcal{B}$:

$$\nu_n^x(B) = \tfrac{1}{n} \left(\textstyle\sum_{i=1}^n \mathbb{1}_B(x_i)\right) \text{ et } \mu_n^x(B) = \tfrac{1}{n} \left(\textstyle\sum_{i=1}^n Y_i \mathbb{1}_B(x_i)\right).$$

Par ailleurs, on pose pour tout $B \in \mathcal{B}$:

$$\nu_n(B) = \tfrac{1}{n} \left(\textstyle\sum_{i=1}^n \mathbb{1}_B(X_i)\right) \text{ et } \mu_n(B) = \tfrac{1}{n} \left(\textstyle\sum_{i=1}^n Y_i \mathbb{1}_B(X_i)\right),$$
$$\nu'_n(B) = \tfrac{1}{n} \left(\textstyle\sum_{i=1}^n \mathbb{1}_B(X'_i)\right).$$

On fixe un entier pair $r \geq 2$.

Soit $\mathcal{V} \subset \mathcal{B}$ une famille dénombrable de parties de X contenant $\emptyset$.
Soient $c \geq 1$ et $\beta \geq 1$. On suppose que $\mathcal{V}$ *possède la propriété* $VC(c, \beta)$, c'est à dire que, pour chaque loi de probabilité Q sur $(X, \mathcal{B})$, toute partie ε-discernable de $\mathcal{V}$ (lorsque $\mathcal{V}$ est muni de la distance $d_Q : (V, T) \longmapsto Q(V \, \Delta \, T)$) est de cardinal inférieur ou égal à $c\varepsilon^{-\beta}$, quel que soit $\varepsilon \in]0, 1]$.

On en verra des exemples dans la partie IV.

On se propose de démontrer que la quantité $\| \sup_{V \in \mathcal{V}} \sqrt{n} \, |\nu_n(V) - P(V)| \|_r$ reste bornée indépendamment de n et de P.
1. Soit q tel que $\frac{1}{q} + \frac{1}{r} = 1$. Montrer que, pour tout $y \in \mathbb{R}$,

$$\sup_{t \in \mathbb{R}} (ty - \frac{|t|^q}{q}) \text{ vaut } \frac{|y|^r}{r}.$$

2. Déduire de la question précédente que, pour tout $x \in X^n$,

$$\sup_{V \in \mathcal{V}} |\nu_n^x(V) - P(V)|^r \text{ est majoré par } \mathbb{E}(\sup_{V \in \mathcal{V}} |\nu_n^x(V) - \nu'_n(V)|^r).$$

On pose $D_n = \| \sup_{V \in \mathcal{V}} |\nu_n(V) - P(V)| \|_r$; montrer l'inégalité suivante:

$$D_n^r \leq \mathbb{E}(\sup_{V \in \mathcal{V}} |\nu_n(V) - \nu'_n(V)|^r).$$

3. Posons $Z_i = \mathbb{1}_V(X_i) - \mathbb{1}_V(X_i')$ pour $i = 1, \cdots, n$; montrer que $(Z_1, \cdots, Z_n)$ a même loi que $(Y_1 Z_1, \cdots, Y_n Z_n)$. En déduire l'inégalité suivante:

$$D_n^r \leq \mathbb{E}(\sup_{V \in \mathcal{V}} |\frac{1}{n} (\sum_{i=1}^{n} Y_i(\mathbb{1}_V(X_i) - \mathbb{1}_V(X_i'))|^r)$$

et donc que D_n est majoré par $2\| \sup_{V \in \mathcal{V}} |\mu_n(V)|\|_r$.

4. Fixons $x \in X^n$; montrer l'inégalité suivante:

$$\|\sqrt{n}\ (\mu_n^x(V) - \mu_n^x(T))\|_r \leq \sqrt{r}\sqrt{\nu_n^x(V \,\Delta\, T)}.$$

5. Fixons $x \in X^n$; on munit $\mathcal{V}$ de la distance

$$d_{(r)} : (V, T) \mapsto \|\sqrt{n}\ (\mu_n^x(V) - \mu_n^x(T))\|_r.$$

Montrer que toute partie ε-discernable de $\mathcal{V}$ (lorsque $\mathcal{V}$ est muni de la distance $d_{(r)}$) est de cardinal inférieur ou égal à $c_0 \varepsilon^{-\beta_0}$ (avec $c_0 = cr^\beta$ et $\beta_0 = 2\beta$), quel que soit $\varepsilon \in]0, \sqrt{r}]$.

6. Fixons $x \in X^n$; on pose

$$A_n^x = \| \sup_{V \in \mathcal{V}} \sqrt{n}\ |\mu_n^x(V)|\|_r \text{ et } \delta_n^x = \sup_{V,T \in \mathcal{V}} \nu_n^x(V \,\Delta\, T).$$

Montrer que, dès que $r > 4\beta$,

$$A_n^x \text{ est majoré par } 5c^{1/r}\sqrt{r}\ (\delta_n^x)^{(1/2)-(\beta/r)}.$$

7. Montrer que la quantité $\| \sup_{V \in \mathcal{V}} \sqrt{n}\ |\nu_n(V) - P(V)|\|_r$ est majorée par $10c^{1/r}\sqrt{r}$ dès que $r > 4\beta$.

8. On se place sur $X = \mathbb{R}$; trouver un ensemble dénombrable $\mathcal{T}$ de parties de $\mathbb{R}$ tel que la quantité $\| \sup_{T \in \mathcal{T}} \sqrt{n}\ |\nu_n(T) - P(T)|\|_s$ soit égale à $\sqrt{n}$ (pour tout nombre réel $s \geq 1$) dès que P est une loi de probabilité diffuse sur $\mathbb{R}$, c'est à dire dès que $P(A)$ est nul pour tout A fini.

Quatrième Partie

Soit X un ensemble muni de la tribu $\mathcal{B}$. Si $\mathcal{V} \subset \mathcal{B}$ est une famille de parties de X, et si A est une partie finie de X, on note $\mathcal{V} \cap A$ l'ensemble des parties de A de la forme $V \cap A$ avec $V \in \mathcal{V}$; on dit que A est *pulvérisée* par $\mathcal{V}$ si $\mathcal{V} \cap A$ est l'ensemble de toutes les parties de A; on note $\mathrm{Dim}(\mathcal{V})$ la borne supérieure de $\#(A)$, pour les $A \subset X$ pulvérisés par $\mathcal{V}$.

On se propose de montrer que, si $\mathrm{Dim}(\mathcal{V}) = D$, alors, pour tout $\beta > D$, il existe $c \in]0, +\infty[$ tel que $\mathcal{V}$ ait la propriété $VC(c, \beta)$.

Cela permettrait d'appliquer à $\mathcal{V}$ les résultats de la partie III.

1. Soit A une partie finie de X avec $\#(A) = n$.

(a) Soit $\mathcal{T}$ un ensemble de parties de A. Pour chaque $T \in \mathcal{T}$ et chaque $a \in A$, on pose $T_a^{\mathcal{T}} = T \setminus \{a\}$ si $T \setminus \{a\} \notin \mathcal{T}$, et $T_a^{\mathcal{T}} = T$ sinon. On note $\mathcal{T}_a$ l'ensemble des $T_a^{\mathcal{T}}$ pour $T \in \mathcal{T}$. Montrer qu'on a:

$$\#(\mathcal{T}_a) = \#(\mathcal{T}) \text{ et } \mathrm{Dim}(\mathcal{T}_a) \leq \mathrm{Dim}(\mathcal{T}).$$

(b) Montrer qu'on peut construire un ensemble $\mathcal{U}$ de parties de A, avec:

$$\#(\mathcal{U}) = \#(\mathcal{T}) \text{ et } \mathrm{Dim}(\mathcal{U}) \leq \mathrm{Dim}(\mathcal{T}),$$
$$U_a^{\mathcal{U}} = U \text{ pour tout } U \in \mathcal{U} \text{ et tout } a \in A.$$

En déduire que chaque $U \in \mathcal{U}$ est de cardinal inférieur ou égal à $\mathrm{Dim}(\mathcal{U})$.

(c) Soit $\mathcal{V} \subset \mathcal{B}$ une famille de parties de X, avec $\mathrm{Dim}(\mathcal{V}) = D$. En appliquant (b) à $\mathcal{T} = \mathcal{V} \cap A$, montrer l'inégalité suivante:

$$\#(\mathcal{V} \cap A) \leq \sum_{i=1}^{D} \frac{n!}{i!(n-i)!}.$$

2. Montrer que, pour tout $n \geq D$,

$$\sum_{i=1}^{D} \frac{n!}{i!(n-i)!} \text{ est majoré par } (en/D)^D.$$

Si $\mathcal{V} \subset \mathcal{B}$ est une famille de parties de X, avec $\mathrm{Dim}(\mathcal{V}) = D$, en déduire qu'il existe C fini tel qu'on ait:

$$\#(\mathcal{V} \cap A) \leq C(\#(A))^D \text{ pour tout } A \text{ fini inclus dans } X.$$

3. Soient $X_1, \cdots, X_n$ des v.a. sur $(\Omega, \mathcal{A})$ à valeurs dans $(X, \mathcal{B})$ indépendantes et de loi Q. Montrer qu'on a, pour tout $V, T \in \mathcal{B}$:

$$\mathbb{P}(\{X_1, \cdots, X_n\} \cap V = \{X_1, \cdots, X_n\} \cap T) \leq \exp(-n d_Q(V, T)).$$

En déduire que, si $\mathcal{V}$ est une partie de $\mathcal{B}$ avec $\mathrm{Dim}(\mathcal{V}) = D < +\infty$ et si $V_1, \cdots, V_N$ sont des éléments distincts de $\mathcal{V}$ vérifiant

$$\sum_{i,j,i \neq j} \exp(-n d_Q(V_i, V_j)) < 1,$$

alors N est inférieur ou égal à Cn^D.

4. Soit $\mathcal{V} \subset \mathcal{B}$ une famille de parties de X, avec $\mathrm{Dim}(\mathcal{V}) = D < +\infty$.
On se donne $\beta > D$, $\varepsilon \in]0, 1]$ et une loi de probabilité Q sur $(X, \mathcal{B})$. Soient $V_1, \cdots, V_N$ $(N \geq 2)$ des éléments de $\mathcal{V}$ avec $d_Q(V_i, V_j) > \varepsilon$ pour tous i,j distincts.
Montrer qu'il est possible de choisir $c \geq 1$ tel que l'on ait

$$C(4\ln(N))^D \leq c^{D/\beta}\, N^{1-(D/\beta)} \text{ pour tout } N \geq 2.$$

Montrer qu'alors N est inférieur ou égal à $c\varepsilon^{-\beta}$
(pour cela prendre pour n le plus petit entier $> (2/\varepsilon)\ln(N)$).
En déduire que $\mathcal{V}$ a la propriété $VC(c, \beta)$.

5. On appelle demi-espace affine dans $\mathbb{R}^2$, toute partie de la forme
$\{(x_1, x_2) \in \mathbb{R}^2 \mid u_1 x_1 + u_2 x_2 > v\}$ (avec u_1, u_2 et v dans $\mathbb{R}$).
Soit $\mathcal{V}$ l'ensemble des demi-espaces affines dans $\mathbb{R}^2$.
Montrer que $\mathrm{Dim}(\mathcal{V})$ est égale à 3.

6. Soit $\mathcal{V}$ l'ensemble de toutes les parties convexes de $\mathbb{R}^2$.
Montrer que $\mathrm{Dim}(\mathcal{V})$ est infinie.

MATHÉMATIQUES DE L'INFORMATIQUE

Le but du problème est d'étudier des codes correcteurs d'erreurs. Ils sont utilisés pour rendre plus fiables les transmissions numériques en permettant de détecter et de corriger certaines erreurs.

I. Notations et définitions

Étant donné un ensemble E, on notera $|E|$ le nombre de ses éléments.

On notera $\mathbb{F}_q$ le corps à q éléments, où q est une puissance d'un nombre premier p et $\mathbb{F}_q^*$ l'ensemble des éléments inversibles de $\mathbb{F}_q$. On écrira les éléments de $\mathbb{F}_2$: 0, 1 sans distinction avec les nombres entiers naturels.

On appelle *mots* de longueur n les éléments de l'espace vectoriel $(\mathbb{F}_q)^n$. On les notera sous la forme de vecteurs ligne $(x_1, \ldots, x_n)$ ou $(x_0, \ldots, x_{n-1})$ selon le contexte.

À tout $x = (x_1, \ldots, x_m)$ dans $(\mathbb{F}_2)^m$ on fait correspondre le nombre entier $N_m(x)$ dont les x_i sont les composantes du développement binaire

$$N_m(x) = \sum_{i=1}^{m} x_i 2^{i-1}.$$

Ainsi N_m est une bijection de $(\mathbb{F}_2)^m$ sur $\{0, 1, \ldots, 2^m - 1\}$. On désigne par M_m l'application réciproque de N_m.

On identifiera un polynôme avec la famille finie de ses coefficients.

Définition. *Un code C de longueur n sur le corps $\mathbb{F}_q$ est un sous-espace vectoriel de $(\mathbb{F}_q)^n$. Les éléments de C sont appelés mots du code. La dimension du code est sa dimension comme sous-espace vectoriel.*

Une *matrice génératrice* d'un code C de longueur n et de dimension k est une matrice à k lignes et n colonnes dont les lignes engendrent le code. Si G est une matrice génératrice d'un code C de longueur n et de dimension k, l'application qui à un mot a de $(\mathbb{F}_q)^k$ fait correspondre le mot aG dans $(\mathbb{F}_q)^n$ est dite *application d'encodage*. On dit que la matrice génératrice G est *de forme canonique* si elle s'écrit par blocs : $G = \left(I_k \ \vdots \ P\right)$ où I_k est la matrice unité de rang k et P est une matrice à k lignes et $n - k$ colonnes.

Une *matrice de contrôle* H est une matrice à $n - k$ lignes et n colonnes telle qu'un mot c soit dans C si et seulement si $H\,c^\top = 0$ en notant $c^\top$ la transposée de la matrice ligne c.