SPÉCIALE MP* : DEVOIR SURVEILLÉ

Partie I

I.1. **a.** On a $W(a) = 0 \Leftrightarrow a = 0$ (a a toutes ses composantes nulles) donc $\Delta(x, y) = 0 \Leftrightarrow x = y$. Puis $W(-a) = W(a)$ soit $\Delta(x, y) = \Delta(y, x)$.
Enfin, $W(a + b) \leqslant W(a) + W(b)$ car le nombre de composantes nulles de a additionné à celles de b est inférieur ou égal au nombre de composantes non nulles de $a + b$ d'où $\Delta(x, y) = W(x - y) = W(w - z + z - y) \leqslant W(x - z) + W(z - y)$. 2

b. Soit $t = \left[\frac{d-1}{2}\right]$, s'il existe 2 éléments x_1, x_2 de C tels que $\Delta(x_1, y) \leqslant t, \Delta(x_2, y) \leqslant t$ alors $\Delta(x_1, x_2) \leqslant 2t$ i.e. $W(x_1 - x_2) \leqslant 2\left[\frac{d-1}{2}\right] < d$ ce qui est impossible pour $x_1 - x_2 \neq 0$ car $x_1 - x_2 \in C$ sous-espace vectoriel de F donc $x_1 = x_2$. 3

I.2. **a.** On a $\boxed{\mathrm{Rg}(h(f_i)) = \dim h(F) = \dim F - \dim C = n - k}$ (formule du rang). 2

b. On a $x = \sum\limits_{i \in J} \lambda_i f_i$ donc $h(x) = 0 = \sum\limits_{i \in J} \lambda_i h(f_i)$, $\lambda_i \neq 0$ c.q.f.d. 2

c. On choisit x tel que $\min\limits_{u \in C \setminus \{0\}} W(u) = W(x)$ et on applique le **b**. 2

d. En effet, s'il existe une famille de $d - 1$ vecteurs liée extraite de la famille $(h(f_i))$ alors $\sum\limits_{i \in J} \lambda_i h(f_i) = 0 \Rightarrow x = \sum\limits_{i \in J} \lambda_i f_i \in C \setminus \{0\}$ et $W(x) \leqslant d - 1$ ce qui est absurde. On a donc $\mathrm{rg}\,(h(f_i)) \geqslant d - 1$ i.e. $\boxed{d \leqslant n - k + 1}$. 4

I.3. **a.** C'est un résultat du cours : on utilise le théorème de l'échange.
On peut aussi faire la démonstration suivante : soit J tel que $(h(f_i))_{i \in J}$ soit une base de $h(F)$, (f_i) est une famille libre de $n - k$ éléments. $D = \mathrm{Vect}(f_i)_{i \in J}$ est en somme directe avec C car $D \cap C = \{0\}$ (si $x \in D \cap C$ alors $x = \sum\limits_{i \in J} \lambda_i f_i$ et $h(x) = 0$ entraîne $x = 0$) et $\dim D + \dim C = n$. Comme $\mathrm{Card}\, J = n - k$, $P = J$ répond à la question. 2

b. Si $x \in C$, on écrit $x = \sum\limits_{i=1}^{n} \lambda_i(x) f_i$. Soit : $p \ : x \in C \mapsto \sum\limits_{i=1}^{k} \lambda_i(x) f_i \in D'$ supplémentaire de D. p est injective ($p(x) = 0 \Leftrightarrow x \in C \cap \mathrm{Vect}(f_{k+1}, \ldots, f_n) = \{0\}$) donc bijective car $\dim C = \dim D'$.
On peut alors prendre la base $\mathcal{B}'_E = (e'_1, \ldots, e'_k)$ où e'_i est l'unique vecteur de E vérifiant $g(e'_i) = p^{-1}(f_i)$. 4

c. $D = \mathrm{Vect}(f_{k+1}, \ldots, f_n)$ et $C \oplus D = F$. $\mathrm{Ker}\, h = C$ donc h est bien une application de contrôle. 1
Ensuite, $f_1 = \underbrace{\lambda_1 g(e'_1) + \cdots + \lambda_k g(e'_k)}_{\in C} + \underbrace{\lambda_{k+1} f_{k+1} + \cdots + \lambda_n f_n}_{\in D}$. Si on examine les composantes sur $f_1, f_2, \ldots, f_k$, compte tenu de l'écriture de la matrice G, on peut dire que $\lambda_2 = \ldots = \lambda_k = 0$ et $\lambda_1 = 1$, de même pour $i = 2, \ldots, k$. Si $A = (a_{ij})_{i \in [\![1, n-k]\!], j \in [\![1, k]\!]}$ alors $f_i = g(e'_i) - \sum\limits_{j \geqslant k+1} a_{ij} f_j$ pour $i \leqslant k$, donc $h(f_i) = -\sum\limits_{j=k+1}^{n} a_{ij} h(f_j)$ et comme $h(f_j) = f_j$ pour $j \geqslant k + 1$, la matrice de h s'écrira :

$$H = \begin{pmatrix} -A & I_{n-k} \end{pmatrix}.$$ 3

d. On peut écrire $y = x + e = g(u) + e$ où e représente les erreurs de transmission. On a alors par hypothèse : $W(e) \leqslant t$ et, comme $x \in C$, $h(x) = 0$ donc $h(e) = h(y) = z$... 2

La suite est une conséquence du **1.b**. 1

I.4. a. On a $H = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$ car $-1 = +1$ dans $\mathbb{K}$. 1

b. $n = 7$, $k = 4$ donc $d \leqslant 4 = n - k + 1$. La famille $(h(f_1), h(f_6), h(f_7))$ est liée, donc, en vertu du **2.c** et **d** : $d \leqslant 3$ et comme toute famille de deux vecteurs est libre, on a : $\boxed{d = 3}$. 2

c. $h(y) = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$. Soit $e = (0,0,0,1,0,0,0)$ alors $h(e) = h(y)$, $w(e) = 1$ et l'unique élément de C tel que $W(x,y) \leqslant 1$ est $x = (1,0,1,1,0,1,0)$. 2

On trouve alors $\boxed{u = (1,0,1,1)}$. 1

PARTIE II

II.1. a. On a immédiatement $\mathrm{Card}\, E_k = \mathrm{Card}\, \mathbb{K}^k = 2^k$ et $\mathrm{Card}\, F_k = 2^{2^m}$ en utilisant la propriété $\mathrm{Card}(\mathcal{F}(E,F)) = (\mathrm{Card}\, F)^{\mathrm{Card}\, E}$. 3

Comme tout espace vectoriel de dimension p sur $\mathbb{K} = \{0,1\}$ contient 2^p éléments, on en déduit que $\boxed{\dim F_k = 2^m}$. 3

b. Si $x \in [\![0, 2^m - 1]\!]$ alors $x = w_1 + w_2.2 + \cdots + w_m.2^{m-1}$ (écriture en base 2 qui est unique) ce qui permet de définir α^{-1} et de conclure. 2

c. A un nombre écrit en base 2, on fait correspondre le sous-ensemble de $[\![1, m]\!]$ correspondant à la position de ses chiffres dans l'écriture en base 2. Là encore, on a bien une bijection. 2

d. Comme $\dim F_k = 2^m$, il suffit de prouver que $(f_0, \ldots, f_{2^m-1})$ est libre. Soit $\sum\limits_{j=0}^{2^m-1} \lambda_j f_j = 0$ alors en appliquant ceci à $(v_1, \ldots, v_m) = \alpha^{-1} \circ \beta^{-1}(P_i)$ on a $\lambda_i = 0$. 2

e. On a $f_j(\alpha^{-1} \circ \beta^{-1}(P_i)) = 0$ si $i \neq j$, $= 1$ si $i = j$ donc $\boxed{f_j = \prod\limits_{i \in P_j} V_i . \prod\limits_{i \notin P_j} \overline{V_i}}$. 3

f. On a immédiatement $f = \sum\limits_{j=0}^{2^m-1} f(\alpha^{-1}(j)).f_j$ et $U = \sum\limits_{j=0}^{2^m-1} f_j$. 2

Pour $k = 2$, $V_1 = f_1$, pour $k = 3$, $V_1 = (0,1,0,1)$, $V_2 = (0,0,1,1)$, ... 1

et pour $k = 4$, $V_1 = (0,1,0,1,0,1,0,1)$, $V_2 = (0,0,1,1,0,0,1,1)$,
$V_3 = (0,0,0,0,1,1,1,1)$. 2

Par un raisonnement semblable on obtient

$$\begin{aligned} V_i &= (f_{2^{i-1}} + \cdots + f_{2^i-1}) + \cdots + (f_{2^m-2^i} + \cdots + f_{2^m-1}) \\ &= \sum_{h=0}^{2^{m-i}} \sum_{k=2^i.h+2^{i-1}}^{2^i.h+2^i-1} f_k = \sum_{h=0}^{2^{m-i}} \sum_{k=0}^{2^{i-1}-1} f_{2^{i-1}(2h+1)+k}. \end{aligned}$$ 3

II.2. a. Il est immédiat que g_k est linéaire.

Pour montrer que g_k est injective, il suffit de prouver que $U, V_1, \ldots, V_m$ est libre.

Soit $\lambda_0 U_0 + \lambda_1 V_1 + \cdots + \lambda_m V_m = 0$ alors, en cherchant l'image par cette application des vecteurs $(0,0,\ldots,0), (1,0,\ldots,0)$ et $(0,0,0,\ldots,1)$, on trouve :

$\lambda_0 = 0$, $\lambda_0 + \lambda_1 = 0$,...$\lambda_0 + \lambda_m = 0$ d'où $\lambda_0 = \lambda_1 = \ldots = \lambda_m = 0$ donc g_k est bien injective. 2

b. $\boxed{k=2}$, $m=1$, $\mathcal{B}_{F_2}=(f_0,f_1)$, $U=f_0+f_1$, $V_1=f_1$, $C_2=F_2$, $d_2=1$. . . . . $\boxed{1}$

$\boxed{k=3}$, $m=2$, $\mathcal{B}_{F_3}=(f_0,f_1,f_2,f_3)$, $\begin{cases} U=f_0+f_1+f_2+f_3 \\ V_1=f_1+f_3 \\ V_2=f_2+f_3 \end{cases}$.

$x\in C_3 \Leftrightarrow x=u_0f_0+(u_0+u_1)f_1+(u_0+u_2)f_2+(u_0+u_1+u_2)f_3 \Leftrightarrow x_0+x_3=x_1+x_2$.

$\boxed{d_3=2}$: en effet, si x a 3 composantes nulles ($W(x)=1$) alors la $4^{\text{ième}}$ est nulle grâce à la relation que l'on vient de prouver. On a alors $d_3\geqslant 2$ et comme $(1,0,1,0)\in C_2$ alors $d_3=2$. . . . . $\boxed{1}$

c. Si $j\leqslant 2^{m-1}$ alors $P_j=\operatorname{supp}(v_1,\dots,v_{m-1},0)$ et $P_{j+2^{m-1}}=\operatorname{supp}(v_1,\dots,v_{m-1},1)$. On met alors en évidence une partition de l'ensemble des parties de $[\![1,m]\!]$.

Si

$$\begin{aligned} x &= u_0U+u_1V_1+\cdots+u_{m-1}V_{m-1} \\ &= x_0f_0+\cdots+x_{2^{m-1}-1}f_{2^{m-1}-1}+x_{2^{m-1}}f_{2^{m-1}}+\cdots+x_{2^m-1}f_{2^m-1} \end{aligned}$$

alors $x_j=x_{j+2^{m-1}}$ car on trouve exactement les mêmes termes dans leur somme. Les 2^{m-1} premières composantes sont donc égales aux 2^{m-1} dernières et elles sont en fait égales à celles de $g_{k-1}(u_0,\dots,u_{m-1})$ (compte tenu de l'écriture des V_i du **1.f**). . . . . . $\boxed{3}$

$g_k(u_0,\dots,u_{m-1},1)=u_0U+u_1V_1+\cdots+u_{m-1}V_{m-1}+V_m$, or $V_m=f_{2^{m-1}}+\cdots+f_{2^m-1}$ donc

$$g_k(u_0,u_1,\dots,u_{m-1},1)=x_0f_0+\cdots+x_{2^{m-1}-1}f_{2^{m-1}-1}+(1+x_0)f_{2^{m-1}}+\cdots+(1+x_{2^{m-1}-1})f_{2^m-1}.$$

On a exactement 2^{m-1} composantes non nulles car dans $\mathbb{K}$, si $x_i=0$ ou 1 alors $x_1+1=1$ ou 0. . . . . $\boxed{2}$

Si $x\in C_k$ alors on a deux cas :

$x=u_0U+\cdots+u_{m-1}V_{m-1}$ et donc $W(x)\geqslant 2d_{k-1}$ et $\exists x_k|W(x_k)=2d_{k-1}$,

$x=u_0U+\cdots+u_{m-1}V_{m-1}+V_m$ et dans ce cas, $W(x)=2^{m-1}$.

On a alors $d_k=\min(2d_{k-1},2^{m-1})$ et par récurrence :

$$\boxed{d_k=2^{m-1}=2^{k-2}.} \qquad \boxed{3}$$

II.3. a. $\chi(w)^2=\chi(2w)$ or, sur $\mathbb{K}$, $2w=0$ donc $\chi(w)^2=1$. . . . . $\boxed{1}$

On pose ensuite $\chi(e_i)=(-1)^{v_i}$ où $v_i\in\{0,1\}$ et $v=\sum_{i=1}^m v_ie_i$ alors $\chi=\chi_v$ car χ est déterminé de manière unique par les valeurs qu'il prend sur les vecteurs de base. . . $\boxed{2}$

b. $v\neq 0$ alors soit i tel que $v_i\neq 0$ ($v_i=1$), on prend $s=e_i$. . . . . $\boxed{0}$

Ensuite $(\chi_v|\chi_0)=\sum_{w\in\mathbb{K}^m}\chi_v(w)=\sum_{w\in\mathbb{K}^m}\chi_v(w+s)=-\sum_{w\in\mathbb{K}^m}\chi_v(w)=0$ c.q.f.d. . . . . $\boxed{3}$

c. $(\chi_v|\chi_v)=\sum_{w\in\mathbb{K}^m}\chi_v(w)^2=2^m$ donc $\|\frac{1}{2^{m/2}}\chi_v\|=1$ et si $u\neq v$,

$(\chi_u|\chi_v)=\sum_{w\in\mathbb{K}^m}\chi_u(w)\chi_v(w)=\sum_{w\in\mathbb{K}^m}\chi_{u+v}(w)=0$ c.q.f.d. . . . . $\boxed{2}$

d. $\widehat{\varphi}(v)=(\varphi|\chi_v)$ donc (1) est l'écriture de φ dans une base orthonormale. . . . . $\boxed{1}$

(2) : $2^{2m}(\varphi|\varphi)=\sum_{(v,v',w)\in(\mathbb{K}^m)^3}\widehat{\varphi}(v)\widehat{\varphi}(v')\chi_v(w)\chi_{v'}(w)=\sum_{(v,v')\in(\mathbb{K}^m)^2}\widehat{\varphi}(v)\widehat{\varphi}(v')\times\left(\sum_{w\in\mathbb{K}^m}\chi_v(w)\chi_{v'}(w)\right)$.

Comme cette dernière quantité vaut $2^m\delta_{vv'}$ on en déduit

$$\boxed{(\varphi|\varphi)=\frac{1}{2^m}\sum_{v\in\mathbb{K}^m}\widehat{\varphi}(v)=\frac{1}{2^m}(\widehat{\varphi}|\widehat{\varphi}).} \qquad \boxed{3}$$

(3) : on remarque que

$$\widehat{\widehat{\varphi}}(v) = (\widehat{\varphi}|\chi_v) = \sum_{w\in\mathbb{K}^m} \widehat{\varphi}(w)\chi_v(w) = \sum_{w\in\mathbb{K}^m} (\varphi|\chi_w)\chi_v(w) = \sum_{(w,u)\in(\mathbb{K}^m)^2} \varphi(u)\chi_w(u)\chi_v(w)$$

$$= \sum_{u\in\mathbb{K}^m} \varphi(u)\left(\sum_{w\in\mathbb{K}^m} \chi_u(w)\chi_v(w)\right) = 2^m\varphi(v) \text{ car } \chi_u(w) = \chi_w(u).$$ 2

$\mathcal{F}$ est donc une isométrie (2), involutive (3). 1

On a enfin : $\mathcal{F}(\chi_v)(w) = 2^{-m/2}\left(\dfrac{\chi_v}{2^{m/2}}\Big|\chi_w\right) = \delta_{vw}$. 1

II.4. **a.** $\varphi_{V_i}(w) = (-1)^{V_i(w)} = (-1)^{w_i} = (-1)^{<e_i|w>}$, il suffit donc de prendre $v = e_i$, $\varphi_{V_i} = \chi_{e_i}$. Compte tenu du **3.c**, on aura :

$$\boxed{\widehat{\varphi_{V_i}}(w) = 2^m\delta_{e_iw}}.$$ 2

Ensuite $U(w) = 1$ donc $\varphi_U(w) = -1$ d'où

$$\boxed{\widehat{\varphi_U}(v) = (\varphi_U|\chi_v) = -\sum_{w\in\mathbb{K}^m}\chi_v(w) = -2^m\delta_{v0}.}$$ 1

b. On a $\widehat{\varphi}_f(v) = \sum_{w\in\mathbb{K}^m}\varphi_f(w)\chi_v(w) = \sum_{w\in\mathbb{K}^m}(-1)^{f(w)+\sum_{i=1}^m v_iw_i}$.

Or $V_i(w) = w_i$ donc $f(w) + \sum_{i=1}^m v_iw_i = \left(f + \sum_{i=1}^m v_iV_i\right)(w)$. Si $f + \sum_{i=1}^m v_iV_i = \sum_{j\in A} f_j$ alors le produit $(-1)^{\sum_{j\in A} f_j(w)} = \prod_{j\in A}(-1)^{f_j(w)}$ est égal à 1 sauf si $\alpha(w) = j$ et dans ce cas, il vaut -1.

Quand on fait la somme sur $\mathbb{K}^m$, pour chaque j de A, il y a un seul $W \in \mathbb{K}^m$ tel que $\alpha(w) = j$ donc $\widehat{\varphi}_f(v) = \sum_{\alpha(w)\notin A} + \sum_{\alpha(w)\in A} -1$ ce qui est bien le résultat demandé ! 4

Soit λ_0 le nombre de composantes non nulles et λ_1 celui des composantes nulles. On a $\begin{cases}\lambda_0 + \lambda_1 = 2^m\\ \lambda_0 - \lambda_1 = \widehat{\varphi_f}(v)\end{cases}$ d'où $\lambda_1 = \dfrac{1}{2}(2^m - \widehat{\varphi_f}(v)) = W\left(f + \sum_{i=1}^m v_iV_i\right) = W\left(f - \sum_{i=1}^m v_iV_i\right)$ car, comme $\mathbb{K} = \mathbb{Z}_2$, $\sum_{i=1}^m v_iV_i = -\sum_{i=1}^m v_iV_i$. 2

On démontre alors que $\widehat{\varphi_f}(v)$ est égal au nombre de composantes non nulles de $f + U + \sum_{i=1}^m v_iV_i$ diminué du nombre de composantes nulles (rajouter U revient à transformer une composante nulle en une composante non nulle et vice-versa), d'où :

$$\boxed{\Delta(f, U + \sum_{i=1}^m v_iV_i = \frac{1}{2}(2^m + \widehat{\varphi_f}(v)}.$$ 1

c. On calcule les V_i : $V_1 = f_1 + f_3 + f_5 + f_7 = (0,1,0,1,0,1,0,1)$ dans la base des f_i, $V_2 = (0,0,1,1,0,0,1,1)$ et $V_3 = (0,0,0,0,1,1,1,1)$ et par un calcul un peu long ...

v	(0,0,0)	(1,0,0)	(0,1,0)	(1,1,0)	((0,0,1)	(1,0,1)	(0,1,1)	(1,1,1)
$\widehat{\varphi_f}(v)$	-2	-2	2	2	2	2	6	2

. 3

On a alors $\Delta(f, V_2 + V_3) = \dfrac{1}{2}(8-6) = 1$ et ceci réalise le minimum. 1

Conclusion $x = V_2 + V_3$ et $u = (0,0,1,1)$. 1