Devoir libre 7 (facultatif)
Eléments de correction

Première partie

1. a. On a $A\Delta\emptyset = A$ et $A\Delta E = E \setminus A$ d'où $d(A,\emptyset) = \operatorname{Card} A$ et $d(A,E) = n - \operatorname{Card} A$.
b. On a $(A\Delta B)\Delta\emptyset = A\Delta B$ d'où $d(A\Delta B,\emptyset) = d(A,B)$.

2. a. En dressant les tables de z_i et $|x_i - y_i|$ (en fonction de x_i et y_i), on constate que ces deux quantités sont égales.
b. En notant $(x_i)_{i=1}^n$, $(y_i)_{i=1}^n$ et $(z_i)_{i=1}^n$ les n-uplets représentant les parties A, B et C, l'inégalité triangulaire dans $\mathbb{R}$ amène :

$$\begin{aligned} d(A,C) &= \sum_{i=1}^n |x_i - z_i| = \sum_{i=1}^n |(x_i - y_i) - (z_i - y_i)| \\ &\leqslant \sum_{i=1}^n |x_i - y_i| + \sum_{i=1}^n |z_i - y_i| = d(A,B) + d(B,C). \end{aligned}$$

Deuxième partie

1. a. Étant donnés deux éléments $y = \sum_i \varepsilon_i x_i$ et $y' = \sum_i \varepsilon'_i x_i$ de $\mathscr{C}$, le vecteur $y + y' = \sum_i (\varepsilon_i + \varepsilon'_i) x_i$ appartient à $\mathscr{C}$. Comme $\mathscr{C}$ est non vide (il contient O), c'est donc un code.
On observe par ailleurs que $x_3 = x_1 + x_2$ si bien que tout élément $y = \sum_i \varepsilon_i x_i$ de $\mathscr{C}$ s'écrit

$$y = (\varepsilon_1 + \varepsilon_3)x_1 + (\varepsilon_2 + \varepsilon_3)x_2 + \varepsilon_4 x_4.$$

Il en résulte que

$$\mathscr{C} = \{\varepsilon_1 x_1 + \varepsilon_2 x_2 + \varepsilon_4 x_4\}_{\varepsilon_1,\varepsilon_2,\varepsilon_4 \in \mathbb{K}}.$$

b. Les éléments x_1, x_2, x_3, x_4 et $x_3 + x_4$ étant deux-à-deux distincts, le code $\mathscr{C}$ est constitué d'au moins 5 éléments. Il ne peut donc s'écrire sous la forme $\{\varepsilon_1 u_1 + \varepsilon_2 u_2\}_{\varepsilon_1,\varepsilon_2 \in \mathbb{K}}$ pour $u_1, u_2 \in \mathscr{C}$ puisqu'un tel code est de cardinal inférieur ou égal à 4.
c. C'est immédiat.

2. Les résultats de cette question découlent immédiatement des questions **I.1.b.** et **I.2.b.** en associant à chaque vecteur $x \in \mathbf{M}_{n,1}(\mathbb{K})$ l'ensemble X formé des indices $i \in [\![1, n]\!]$ tels que $x_i \neq 0$: au vecteur $x + y$ correspond alors l'ensemble $X\Delta Y$.

3. a. On remarque pour commencer que toute famille formée d'un unique élément de $\mathscr{C} \setminus \{O\} \neq \emptyset$ est $\mathbb{K}$-libre. Par ailleurs, les éléments d'une famille $\mathbb{K}$-libre sont nécessairement deux-à-deux distincts ; leur nombre ne peut donc excéder le cardinal de $\mathbf{M}_{n,1}(\mathbb{K})$, c'est-à-dire 2^n. Ainsi l'ensemble des cardinaux des familles $\mathbb{K}$-libres d'éléments de $\mathscr{C}$ est une partie non vide et majorée (par 2^n) de $\mathbb{N}$. Il admet à ce titre un plus grand élément p.
Soit $(u_1, \dots, u_p)$ une famille $\mathbb{K}$-libre formée d'éléments de $\mathscr{C}$. Une telle famille ($\mathbb{K}$-libre maximale) est nécessairement une $\mathbb{K}$-base de $\mathscr{C}$. En effet, étant donné un vecteur $y \in \mathscr{C}$, la famille $(u_1, \dots, u_p, y)$ est liée par maximalité de p : il existe $\varepsilon_1, \dots, \varepsilon_p, \eta \in \mathbb{K}$ non tous nuls tels que $\sum_i \varepsilon_i u_i + \eta y = 0$. Le coefficient η ne peut être nul sans quoi on aurait une relation de dépendance linéaire entre les vecteurs $u_1, \dots, u_p$, en contradiction avec l'hypothèse de liberté de la famille $(u_1, \dots, u_p)$. On a donc $\eta = 1$ puis

$$y = y + \left(\sum_i \varepsilon_i u_i + \eta y\right) = \sum_i \varepsilon_i u_i.$$

b. Étant donné $y \in \mathscr{C}$, l'existence d'une décomposition $y = \sum_i \varepsilon_i u_i$ est déjà acquise. S'il en admet une seconde $y = \sum_i \varepsilon'_i u_i$, alors

$$0 = y + y = \sum_i (\varepsilon_i + \varepsilon'_i) u_i$$

d'où, puisque la famille $(u_1, \dots, u_p)$ est $\mathbb{K}$-libre, $\varepsilon_i + \varepsilon'_i = 0$ c'est-à-dire $\varepsilon_i = \varepsilon'_i$ pour tout $i \in [\![1, p]\!]$. L'application $(\varepsilon_i)_i \longmapsto \sum_i \varepsilon_i u_i$ est donc une bijection de $\mathbb{K}^p$ sur $\mathscr{C}$. Le code $\mathscr{C}$ est donc de cardinal 2^p.

c. Puisque l'application $p \longmapsto 2^p$ est injective, toutes les $\mathbb{K}$-bases de $\mathscr{C}$ ont même cardinal d'après la question **b.**.

d. Il s'agit de montrer que le code $\mathscr{C}' = \{\varepsilon_1 v_1 + \cdots + \varepsilon_p v_p\}_{\varepsilon_1,\ldots,\varepsilon_p \in \mathbb{K}}$ est égal à $\mathscr{C}$. Il est tout d'abord inclus dans $\mathscr{C}$ et, comme la famille $\mathbb{K}$-libre $(v_1, \ldots, v_p)$ en est une $\mathbb{K}$-base, il est donc de cardinal 2^p. Le code $\mathscr{C}$ est lui aussi de cardinal 2^p puisqu'il admet une base de cardinal p. On a donc égalité des cardinaux dans l'inclusion $\mathscr{C}' \subset \mathscr{C}$, d'où l'égalité $\mathscr{C}' = \mathscr{C}$.

4. a. C'est immédiat par distributivité du produit sur l'addition matricielle.

b. Il suffit de considérer une permutation σ de $[\![1, n]\!]$ qui, quand on l'applique aux colonnes de Q, transforme Q en $\begin{pmatrix} \mathrm{I}_p & \mathrm{P} \end{pmatrix}$. On notera, contrairement à ce qu'une maladresse de l'énoncé pourrait laisser croire, que la même permutation convient pour tout vecteur x...

c. En notant $\mathrm{P} = (\pi_{i,j})_{1 \leqslant i \leqslant p, p+1 \leqslant j \leqslant n} \in \mathbf{M}_{p,n-p}(\mathbb{K})$, la condition $\mathrm{Q}x = \mathrm{O}$ équivaut d'après **b.** à

$$\forall i \in [\![1, p]\!], \quad x_{\sigma(i)} = \sum_{j=p+1}^{n} \pi_{i,j} x_{\sigma(j)},$$

qui apparaît comme un système linéaire à p équations d'inconnues principales $x_{\sigma(1)}, \ldots, x_{\sigma(p)}$ et d'inconnues secondaires $x_{\sigma(p+1)}, \ldots, x_{\sigma(n)}$. Dans ces conditions, les formules précédentes définissent une application $(x_{\sigma(p+1)}, \ldots, x_{\sigma(n)}) \longmapsto x$ bijective de $\mathbb{K}^{n-p}$ dans $\mathscr{C}_\mathrm{Q}$. Le code est donc de cardinal 2^{n-p}, c'est-à-dire de dimension $n - p$.

d. Un produit par blocs fait apparaître que

$$\mathrm{Q}\begin{pmatrix} \mathrm{I}_{n-p} \\ \mathrm{B} \end{pmatrix} = \begin{pmatrix} \mathrm{B} & \mathrm{I}_p \end{pmatrix}\begin{pmatrix} \mathrm{I}_{n-p} \\ \mathrm{B} \end{pmatrix} = \mathrm{B} + \mathrm{B} = \mathrm{O},$$

si bien que les colonnes de la matrice $\begin{pmatrix} \mathrm{I}_{n-p} \\ \mathrm{B} \end{pmatrix}$ appartiennent toutes à $\mathscr{C}_\mathrm{Q}$. Elles forment une famille $\mathbb{K}$-libre (vu leurs $n - p$ premières lignes) et de cardinal $n - p = \dim \mathscr{C}_\mathrm{Q}$, donc une $\mathbb{K}$-base de $\mathscr{C}_\mathrm{Q}$ d'après **3.d.**.

e. Soit $\delta = \min_{x \in \mathscr{C}_\mathrm{Q} \setminus \{\mathrm{O}\}} d(x, \mathrm{O})$. En notant $\mathrm{C}_1, \ldots, \mathrm{C}_n$ les colonnes de Q, on a $\mathrm{Q}x = x_1\mathrm{C}_1 + \cdots + x_n\mathrm{C}_n$ pour $x = (x_i)_{1 \leqslant i \leqslant n} \in \mathbf{M}_{n,1}(\mathbb{K})$.
Par hypothèse, $\mathrm{Q}x = \mathrm{O}$ implique donc $x = \mathrm{O}$ dès que x admet au plus $r - 1$ composantes non nulles (car la famille formée des colonnes correspondantes de Q est libre), c'est-à-dire dès que $d(x, \mathrm{O}) < r$. Il en résulte que $\delta \geqslant r$.
D'autre part, il existe par hypothèse une relation de liaison entre r colonnes de Q, c'est-à-dire un vecteur $x \in \mathbf{M}_{n,1}(\mathbb{K}) \setminus \{\mathrm{O}\}$ admettant au plus r composantes non nulles, ou encore tel que $d(x, \mathrm{O}) \leqslant r$, vérifiant $\mathrm{Q}x = \mathrm{O}$. Il en ressort que $\delta \leqslant r$.

Troisième partie

1. Parmi les colonnes de H, on trouve les p colonnes de la matrice I_p. Dans ces conditions, la question **II.4.c.** assure que le code $\mathscr{C}_\mathrm{H}$ est de dimension $n - p$.

2. Sachant l'application $(u, v) \longmapsto u + v$ est surjective de $\{(u, v)\}_{u \neq v \in \mathscr{C}_\mathrm{H}}$ dans $\mathscr{C}_\mathrm{H} \setminus \{\mathrm{O}\}$, il vient d'après **II.2.a.** :

$$\min_{u \neq v \in \mathscr{C}_\mathrm{H}} d(u, v) = \min_{u \neq v \in \mathscr{C}_\mathrm{H}} d(u + v, \mathrm{O}) = \min_{w \in \mathscr{C}_\mathrm{H} \setminus \{\mathrm{O}\}} d(w, \mathrm{O}).$$

On détermine alors ce minimum grâce à la question **II.4.e.**. Étant données deux colonnes x et y distinctes de H, on considère $\lambda, \mu \in \mathbb{K}$ tels que $\lambda x + \mu y = 0$. Quitte à échanger x et y, il existe $i \in [\![1, p]\!]$ tel que $x_i = 1$ alors que $y_i = 0$ et $j \in [\![1, p]\!]$ tel que $y_j = 1$. Les relations $\lambda x_i + \mu y_i = 0$ et $\lambda x_j + \mu y_j = 0$ donnent alors $\lambda = \mu = 0$. Ainsi toute famille formée de deux colonnes de H est $\mathbb{K}$-libre. Par ailleurs, si x et y sont deux colonnes distinctes de H, alors $z = x + y$ en est une troisième et la famille (x, y, z) est $\mathbb{K}$-liée puisque $x + y + z = 0$. Il en ressort que $\min_{u \neq v \in \mathscr{C}_\mathrm{H}} d(u, v) = 3$.

3. a. L'ensemble B_v est composé de l'élément v et des n éléments $u \in \mathbf{M}_{n,1}(\mathbb{K})$ qui ne diffèrent de v que par une composante. Il est donc de cardinal $n + 1$.

b. Soient v et w deux éléments distincts de $\mathscr{C}_\mathrm{H}$. Si $u \in \mathrm{B}_v \cap \mathrm{B}_w$, alors $d(v, w) \leqslant d(v, u) + d(u, w) \leqslant 2$ d'après **II.2.b.**, en contradiction avec **2.**. C'est donc que $\mathrm{B}_v \cap \mathrm{B}_w = \emptyset$.

c. L'union $\bigcup_{v\in\mathscr{C}_H} B_v$ étant disjointe d'après **b.**, c'est une partie de $\mathbf{M}_{n,1}(\mathbb{K})$ de cardinal

$$\operatorname{Card}\Big(\bigcup_{v\in\mathscr{C}_H} B_v\Big) = \sum_{v\in\mathscr{C}_H} \operatorname{Card} B_v = (\operatorname{Card}\mathscr{C}_H)(n+1) = 2^{n-p}\cdot 2^p = 2^n = \operatorname{Card}\mathbf{M}_{n,1}(\mathbb{K}),$$

d'où l'égalité $\bigcup_{v\in\mathscr{C}_H} B_v = \mathbf{M}_{n,1}(\mathbb{K})$.

4. a. D'après la question **3.c.**, il existe un unique $v\in\mathscr{C}_H$ tel que $z\in B_v$, c'et-à-dire $d(z,v)\leqslant 1$. Comme $z\notin\mathscr{C}_H$, on a même $z\neq v$ donc $d(z,v)=1$.

b. En notant $e=\Phi(z)+z$, ce qui équivaut à $\Phi(z)=z+e$, la condition $d\big(z,\Phi(z)\big)=1$ devient $d(e,O)=1$ d'après **II.2.a.** et la condition $\Phi(z)\in\mathscr{C}_H$ devient $H(z+e)=0$, c'est-à-dire $Hz=He$. L'existence et l'unicité de e résultent alors directement de **a.**.

5. a. C'est une application directe de la question **II.4.d.**.

b. D'après la question **4.**, le message transmis est $y=\Phi(y^*)=y^*+e$ où e est l'unique vecteur de $\mathbf{M}_{7,1}(\mathbb{K})$ tel que $d(e,O)=1$ (c'est-à-dire l'un des 7 vecteurs de la base canonique) et $H_1y^*=H_1e$. On trouve

$$H_1y^* = \begin{pmatrix}1\\0\\1\end{pmatrix} = H_1e \quad\text{pour}\quad e=\begin{pmatrix}0\\0\\1\\0\\0\\0\\0\end{pmatrix}.$$

Le message transmis est donc

$$y=y^*+e=\begin{pmatrix}0\\1\\1\\0\\1\\1\\0\end{pmatrix} = 0\begin{pmatrix}1\\0\\0\\0\\1\\1\\1\end{pmatrix} + 1\begin{pmatrix}0\\1\\0\\0\\0\\1\\1\end{pmatrix} + 1\begin{pmatrix}0\\0\\1\\0\\1\\0\\1\end{pmatrix} + 0\begin{pmatrix}0\\0\\0\\1\\1\\1\\0\end{pmatrix}.$$

Le message d'origine est donc $(\eta_1,\eta_2,\eta_3,\eta_4)=(0,1,1,0)$.

c. Puisque $d(z,z^*)=2$ avec $z\in\mathscr{C}_{H_1}$, on a $z^*\notin\mathscr{C}_{H_1}$ d'après **2.**. Cela signifie que $H_1z^*\neq 0$, ce qu'il est facile de vérifier par le calcul connaissant z^*, et met en évidence la présence d'une erreur de transmission.

Sachant par ailleurs qu'il y a $\binom{7}{2}=21$ vecteurs $e\in\mathbf{M}_{7,1}(\mathbb{K})$ tels que $d(e,O)=2$, pour lesquels H_1e est l'un des 7 vecteurs non nuls de $\mathbf{M}_{3,1}(\mathbb{K})$, il existe nécessairement deux vecteurs $e_1\neq e_2$ tels que $d(e_1,O)=d(e_2,O)=2$ et $H_1e_1=H_1e_2$. Un même message transmis $z\in\mathscr{C}_{H_1}$ pourra ainsi être reçu sous les deux formes $z_1^*=z+e_1$ et $z_2^*=z+e_2$ avec dans les deux cas deux erreurs de transmission, sans qu'on puisse donc les identifier ni reconstituer le message initial z.

Remarque. Étant donné z^* tel que $H_1z^*\neq O$, on a vu en **4.b.** qu'il existe un unique vecteur $e\in\mathbf{M}_{7,1}(\mathbb{K})$ tel que $d(e,O)=1$ et $H_1z^*=H_1e$. Une analyse du code $\mathscr{C}_{H_1}$ met en évidence qu'il contient 7 éléments u tels que $d(u,O)=3$ et que parmi eux, 3 partagent avec e la même composante non nulle. En les notant u_1, u_2 et u_3, on obtient ainsi trois vecteurs $z_i=z^*+e+u_i$, $1\leqslant i\leqslant 3$, tels que $Hz_i=Hu_i=O$ i.e. $z_i\in\mathscr{C}_{H_1}$ et $d(z_i,z^*)=d(u_i,e)=2$, qui sont donc trois messages pouvant être à l'origine de z^* si la transmission fait intervenir 2 erreurs.

Quatrième partie

1. On notera pour commencer que $k\geqslant 1$ car il y a par hypothèse une unique erreur lors de la transmission, si bien que $Hy^*\neq 0$ d'après **III.2.**. On a par ailleurs $k\leqslant\sum_{i=1}^p 2^{i-1}=2^p-1=n$.

La colonne ${}^t\begin{pmatrix}x_1 & \cdots & x_p\end{pmatrix}$ est précisément la k-ième colonne de H_2 puisque $k=\sum_{i=1}^p x_i2^{i-1}$. Autrement dit, $H_2y^*=H_2e$ où e désigne le k-ième vecteur de la base canonique de $\mathbf{M}_{n,1}(\mathbb{K})$. Comme $d(e,O)=1$, c'est donc que $\Phi(y^*)=y+e$ est le message transmis : l'erreur de transmission s'est produite sur la k-ième composante.

2. a. Il vient :

$$\mathrm{H}_2 = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

On vérifie que les quatre vecteurs d_1, d_2, d_3, d_4 proposés forment une famille libre du code $\mathscr{C}_{\mathrm{H}_2}$, de dimension $n - p = 4$ d'après **III.1.**, et donc une base d'après **II.3.d.**.

b. On note $\bar{x}$, $\bar{y}$ et $\bar{z}$ les trois colonnes transmises. Les colonnes reçues sont quant à elles données par :

$$\bar{x}^* = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}, \quad \bar{y}^* = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} \quad \text{et} \quad \bar{z}^* = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}.$$

On corrige alors les éventuelles erreurs survenues dans chacune des trois transmissions en suivant la méthode décrite en **1.** :

- Le calcul donne $\mathrm{H}_2\bar{x}^* = {}^t\begin{pmatrix} 1 & 1 & 0 \end{pmatrix}$; cette colonne non nulle indique la présence d'une erreur à la composante $1 + 1 \cdot 2 = 3$. Le message transmis est donc

$$\bar{x} = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = 1 \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} + 1 \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} + 0 \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} + 0 \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix},$$

  d'où l'on tire la valeur de $(x_1, x_2, x_3, x_4) = (1, 1, 0, 0)$ puis de $x = 1 + 1 \cdot 2 = 3$.
- Le calcul de $\mathrm{H}_2\bar{y}^* = 0$ montre qu'il n'y a pas eu d'erreur dans la deuxième transmission. On détermine les coordonnées $(y_1, y_2, y_3, y_4) = (1, 0, 0, 0)$ de $\bar{y} = \bar{y}^*$ en base (d_1, d_2, d_3, d_4) pour obtenir la valeur de $y = 1$.
- On calcule de même $\mathrm{H}_2\bar{z}^* = {}^t\begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$, qui indique la présence d'une erreur sur la 7-ième composante. La décomposition du vecteur $\bar{z} = {}^t\begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$ dans la base (d_1, d_2, d_3, d_4) conduit alors à la valeur de $z = 4$.

Primus et Secundus semblent donc sur le point de découvrir le nombre π.

c. Les coordonnées d'un vecteur de $\mathscr{C}_{\mathrm{H}_2}$ dans la base (d_1, d_2, d_3, d_4) étant données par ses quatre première composantes, on peut proposer la fonction suivante (la matrice H_2 étant définie par ailleurs).

Listing 1 : correction des erreurs de transmission et décodage

```
function y=decodage(x)
  C=modulo(H2*x,2); // calcul de H2*x dans K
  if (sum(C)>0) then // en cas d'erreur de transmission
    k=sum(C.*[1;2;4]); // composante erronée
    x(k)=1-x(k);  // correction
  end
  y=sum(x(1:4).*[1;2;4;8]);
endfunction
```

Dans le script précédent, `C` est une colonne dont les coefficients sont des réels égaux à `0` ou `1` ; cette matrice est nulle si, et seulement si, `sum(C)>0` (la somme s'entend dans $\mathbb{R}$, et non dans $\mathbb{K}$).