Partie I L'opération Δ sur les parties d'un ensemble

Q1 a) $d(A,\emptyset) = \text{card}(A\Delta\emptyset) = \text{card}\,A$. $\quad \underline{d(A,\emptyset) = \text{card}\,A}$.

$A\Delta E = (A\cup E)\setminus(A\cap E) = E\setminus A = \overline{A}$. $\quad \underline{d(A,E) = \text{card}\,\overline{A}}$.

b) D'après a) $d(A\Delta B,\emptyset) = \text{card}(A\Delta B) = d(A,B)$. $\quad \underline{d(A,B) = d(A\Delta B,\emptyset)}$.

Q2 a)

$y_i \backslash x_i$	0	1
0	0	1
1	1	0

Table de z_i

$\xleftarrow{z_i}$ $\quad$ $\xrightarrow{|x_i - y_i|}$

$y_i \backslash x_i$	0	1
0	0	1
1	1	0

Table de $|x_i - y_i|$

Les deux tables précédentes montrent que : $\underline{\forall i \in [\![1,n]\!],\ z_i = |x_i - y_i|}$.

__Remarque__.. Il y a autant d'éléments dans $A\Delta B$ que de 1 dans le n-uplet $(z_1, z_2, \ldots, z_n)$. Comme, pour tout i dans $[\![1,n]\!]$, $z_i \in \{0,1\}$ on peut dire que $\text{card}(A\Delta B) = \sum_{i=1}^{n} z_i$.

Ainsi $\underline{d(A,B) = \sum_{i=1}^{n} |x_i - y_i|}$.

{ au sens de la somme de IR !

b) A, B, C sont trois parties de E. Notons $(x_1,\ldots,x_n)$, $(y_1,\ldots,y_n)$, $(z_1,\ldots,z_n)$ les n-uplets "associés".

$\forall i \in [\![1,n]\!]$, $|x_i - z_i| = |(x_i - y_i) + (y_i - z_i)| \leq |x_i - y_i| + |y_i - z_i|$

Alors $\sum_{i=1}^{n} |x_i - z_i| \leq \sum_{i=1}^{n} |x_i - y_i| + \sum_{i=1}^{n} |y_i - z_i|$; $d(A,C) \leq d(A,B) + d(B,C)$.

$\underline{\forall (A,B,C) \in E^3,\ d(A,C) \leq d(A,B) + d(B,C)}$.

Remarques 1.. $\forall a \in K$, $a + a = 0$

2.. Si $\mathcal{B}$ est un code $\forall a \in K$, $\forall x \in \mathcal{B}$, $ax \in \mathcal{B}$. La notion de code correspond à la notion de sous-espace vectoriel.

PARTIE II Une autre algèbre linéaire

(Q1) a) Notons que $\mathcal{C}$ n'est pas vide. Montrons alors que $\forall (x,y)\in \mathcal{C}^2$, $x+y\in\mathcal{C}$.
Soient x et y deux éléments de $\mathcal{C}$. $\exists(\varepsilon_1,\varepsilon_2,\varepsilon_3,\varepsilon_4)\in\mathbb{K}^4$, $x=\varepsilon_1 x_1+\varepsilon_2 x_2+\varepsilon_3 x_3+\varepsilon_4 x_4$.
$\exists(\varepsilon_1',\varepsilon_2',\varepsilon_3',\varepsilon_4')\in\mathbb{K}^4$, $y=\varepsilon_1' x_1+\varepsilon_2' x_2+\varepsilon_3' x_3+\varepsilon_4' x_4$.
$x+y=(\varepsilon_1 x_1+\varepsilon_2 x_2+\varepsilon_3 x_3+\varepsilon_4 x_4)+(\varepsilon_1' x_1+\varepsilon_2' x_2+\varepsilon_3' x_3+\varepsilon_4' x_4)$.
$x+y=(\varepsilon_1 x_1+\varepsilon_1' x_1)+(\varepsilon_2 x_2+\varepsilon_2' x_2)+(\varepsilon_3 x_3+\varepsilon_3' x_3)+(\varepsilon_4 x_4+\varepsilon_4' x_4)$
$x+y=(\varepsilon_1+\varepsilon_1')x_1+(\varepsilon_2+\varepsilon_2')x_2+(\varepsilon_3+\varepsilon_3')x_3+(\varepsilon_4+\varepsilon_4')x_4$. Posons $\forall i\in[\![1,4]\!]$, $\varepsilon_i''=\varepsilon_i+\varepsilon_i'$.
Alors $x+y=\varepsilon_1'' x_1+\varepsilon_2'' x_2+\varepsilon_3'' x_3+\varepsilon_4'' x_4$ avec $(\varepsilon_1'',\varepsilon_2'',\varepsilon_3'',\varepsilon_4'')\in\mathbb{K}^4$. Ainsi $x+y\in\mathcal{C}$.
$\mathcal{C}$ est une partie non vide de $\mathcal{M}_{5,1}(\mathbb{K})$ telle que $\forall(x,y)\in\mathcal{C}^2$, $x+y\in\mathcal{C}$.
<u>$\mathcal{C}$ est un code.</u>

Notons que $x_3=\begin{pmatrix}0\\0\\1\\1\\0\end{pmatrix}=\begin{pmatrix}1+1\\1+1\\0+1\\1+0\\0+0\end{pmatrix}=\begin{pmatrix}1\\1\\0\\1\\0\end{pmatrix}+\begin{pmatrix}1\\1\\1\\0\\0\end{pmatrix}=x_1+x_2$; $\underline{x_3=x_1+x_2}$.

Montrons alors que $\mathcal{C}$ coïncide avec $\widehat{\mathcal{C}}=\{\alpha_1x_1+\alpha_2x_2+\alpha_4x_4,\ (\alpha_1,\alpha_2,\alpha_4)\in\mathbb{K}^3\}$.
Soit $x\in\widehat{\mathcal{C}}$. $\exists(\alpha_1,\alpha_2,\alpha_4)\in\mathbb{K}^3$, $x=\alpha_1x_1+\alpha_2x_2+\alpha_4x_4$.
$x=\alpha_1x_1+\alpha_2x_2+0.x_3+\alpha_4x_4$ et $(\alpha_1,\alpha_2,0,\alpha_4)\in\mathbb{K}^4$, ainsi $x\in\mathcal{C}$.
Réciproquement soit $x\in\mathcal{C}$. $\exists(\varepsilon_1,\varepsilon_2,\varepsilon_3,\varepsilon_4)\in\mathbb{K}^4$, $x=\varepsilon_1x_1+\varepsilon_2x_2+\varepsilon_3x_3+\varepsilon_4x_4$.
$x=\varepsilon_1x_1+\varepsilon_2x_2+\varepsilon_3(x_1+x_2)+\varepsilon_4x_4=(\varepsilon_1+\varepsilon_3)x_1+(\varepsilon_2+\varepsilon_3)x_2+\varepsilon_4x_4$
Posons $\alpha_1=\varepsilon_1+\varepsilon_3$, $\alpha_2=\varepsilon_2+\varepsilon_3$ et $\alpha_4=\varepsilon_4$. $(\alpha_1,\alpha_2,\alpha_4)\in\mathbb{K}^3$ et $x=\alpha_1x_1+\alpha_2x_2+\alpha_4x_4$; $x\in\widehat{\mathcal{C}}$
Finalement $\underline{\mathcal{C}=\{\alpha_1x_1+\alpha_2x_2+\alpha_4x_4,\ (\alpha_1,\alpha_2,\alpha_4)\in\mathbb{K}^3\}}$.

b) Supposons que l'on peut trouver une famille (u_1,u_2) d'éléments de $\mathcal{C}$ telle que $\mathcal{C}=\{\varepsilon_1u_1+\varepsilon_2u_2,\ (\varepsilon_1,\varepsilon_2)\in\mathbb{K}^2\}$. Alors $\mathcal{C}$ a au plus quatre éléments.
Or $x_1=\begin{pmatrix}1\\1\\0\\1\\0\end{pmatrix}$, $x_2=\begin{pmatrix}1\\1\\1\\0\\0\end{pmatrix}$, $x_3=\begin{pmatrix}0\\0\\1\\1\\0\end{pmatrix}$, $x_4=\begin{pmatrix}1\\0\\0\\0\\0\end{pmatrix}$, $x_1+x_4=\begin{pmatrix}0\\1\\0\\1\\0\end{pmatrix}$ sont cinq éléments deux à deux distincts de $\mathcal{C}$ donc $\operatorname{card}\mathcal{C}\geqslant 5$!
<u>Il n'existe pas de famille (u_1,u_2) d'éléments de $\mathcal{C}$ telle que $\mathcal{C}=\{\varepsilon_1u_1+\varepsilon_2u_2,\ (\varepsilon_1,\varepsilon_2)\in\mathbb{K}^2\}$</u>

c] Soit $(\varepsilon_1,\varepsilon_2,\varepsilon_4)\in\mathbb{K}^3$, tel que $\varepsilon_1 x_1+\varepsilon_2 x_2+\varepsilon_4 x_4=0$.

$$\varepsilon_1\begin{pmatrix}1\\1\\0\\1\\0\end{pmatrix}+\varepsilon_2\begin{pmatrix}1\\1\\1\\0\\0\end{pmatrix}+\varepsilon_4\begin{pmatrix}1\\0\\0\\0\\0\end{pmatrix}=0\ ;\quad\begin{pmatrix}\varepsilon_1+\varepsilon_2+\varepsilon_4\\\varepsilon_1+\varepsilon_2\\\varepsilon_2\\\varepsilon_1\\0\end{pmatrix}=0\ ;\quad\left\{\begin{array}{l}\varepsilon_1+\varepsilon_2+\varepsilon_4=0\\\varepsilon_1+\varepsilon_2=0\\\varepsilon_2=0\\\varepsilon_1=0\end{array}\right.\ ;\quad\varepsilon_1=\varepsilon_2=\varepsilon_4=0.$$

$\forall(\varepsilon_1,\varepsilon_2,\varepsilon_4)\in\mathbb{K}^3,\ \varepsilon_1 x_1+\varepsilon_2 x_2+\varepsilon_4 x_4=0\Rightarrow\varepsilon_1=\varepsilon_2=\varepsilon_4=0.$

Q2 a] Soient $x=\begin{pmatrix}x_1\\x_2\\\vdots\\x_n\end{pmatrix}$, $y=\begin{pmatrix}y_1\\y_2\\\vdots\\y_n\end{pmatrix}$ deux éléments de $\mathcal{M}_{n,1}(\mathbb{K})$.

$$d(x,y)\underset{\text{ok!!}}{=}\sum_{i=1}^n|x_i-y_i|=\sum_{i=1}^n|x_i-y_i+\underbrace{y_i+y_i}_{=0}|=\sum_{i=1}^n|x_i\dot{+}y_i|=\sum_{i=1}^n(x_i\dot{+}y_i)=d(x+y,0).$$

$\forall(x,y)\in\mathcal{M}_{n,1}^2(\mathbb{K}),\ d(x,y)=d(x+y,0).$

b] Soient $x=\begin{pmatrix}x_1\\x_2\\\vdots\\x_n\end{pmatrix}$, $y=\begin{pmatrix}y_1\\y_2\\\vdots\\y_n\end{pmatrix}$ et $z=\begin{pmatrix}z_1\\z_2\\\vdots\\z_n\end{pmatrix}$ trois éléments de $\mathcal{M}_{n,1}(\mathbb{K})$.

$$d(x,z)=d(x+z,0)=\sum_{i=1}^n(x_i\dot{+}z_i)=\sum_{i=1}^n[(x_i\dot{+}y_i)\dot{+}(y_i\dot{+}z_i)]\leq\sum_{i=1}^n(x_i\dot{+}y_i)+\sum_{i=1}^n(y_i\dot{+}z_i).$$

A méditer.

$d(x,z)\leq d(x+y,0)+d(y+z,0)=d(x,y)+d(y,z).$

$\forall(x,y,z)\in\mathcal{M}_{n,1}^3(\mathbb{K}),\ d(x,z)\leq d(x,y)+d(y,z).$

Q3 a] Soit $\mathcal{L}$ l'ensemble des familles $\mathcal{X}$ d'éléments de $\mathcal{C}$ telles qu'il existe p dans $\mathbb{N}^*$ et $(x_1,x_2,\dots,x_p)\in\mathcal{C}^p$ avec $\mathcal{X}=(x_1,x_2,\dots,x_p)$ et $(x_1,x_2,\dots,x_p)$ $\mathbb{K}$-libre (... ici le cardinal de la famille est p et non pas le nombre d'éléments de $\{x_1,x_2,\dots,x_p\}$!).

Soit L l'ensemble des cardinaux des familles de $\mathcal{L}$.

Nous allons montrer que L est une partie non vide et majorée de $\mathbb{N}^*$; ainsi L aura un plus grand élément r.

* Etape 1.. Montrons que L n'est pas vide ; il suffit de prouver que $\mathcal{L}$ n'est pas vide.

$\mathcal{E}$ n'est pas réduit à $\{0\}$. $\exists t=\begin{pmatrix} t_1 \\ t_2 \\ \vdots \\ t_n \end{pmatrix} \in \mathcal{E}$ et $t \neq 0$. Montrons que (t) est libre.

Soit $\varepsilon_1 \in \mathbb{K}$ tel que $\varepsilon_1 t = 0$.

$\forall i \in [\![1,n]\!]$, $\varepsilon_1 t_i = 0$. $t \neq 0$ donc $\exists i_0 \in [\![1,n]\!]$, $t_{i_0} \neq 0$.

Comme $t_{i_0} \in \mathbb{K} = \{0,1\}$, $t_{i_0} = 1$. Alors $\varepsilon_1 = 0$.

$\forall \varepsilon_1 \in \mathbb{K}$, $\varepsilon_1 t = 0 \Rightarrow \varepsilon_1 = 0$. (t) est une famille $\mathbb{K}$-libre de $\mathcal{E}$.

$(t) \in \mathcal{L}$. $\mathcal{L} \neq \emptyset$ donc L est une partie non vide de $\mathbb{N}^*$. ■

* Etape 2 Montrons que L est majorée par le cardinal de $\Pi_n(\mathbb{K})$ qui est 2^n.

Soit p un élément de L. Il existe une famille K-libre $(x_1, x_2, \dots, x_p)$ de $\mathcal{E}$.

Le cardinal de cette famille est p. Montrons que p est aussi le cardinal de l'ensemble $\{x_1, x_2, \dots, x_p\}$. Il suffit de montrer que $x_1, x_2, \dots, x_p$ sont deux à deux distincts. Supposons qu'il existe $(i,j) \in [\![1,p]\!]^2$ tel que $i \neq j$ et tel que $x_i = x_j$.

Posons $\forall k \in [\![1,p]\!]$, $\varepsilon_k = \begin{cases} 0 \text{ si } k \notin \{i,j\} \\ 1 \text{ si } k \in \{i,j\} \end{cases}$.

$(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_p) \neq (0,0,\dots,0)$ et $\varepsilon_1 x_1 + \varepsilon_2 x_2 + \dots + \varepsilon_p x_p = \varepsilon_i x_i + \varepsilon_j x_j = x_i + x_j = x_i + x_i = 0$

$\exists (\varepsilon_1, \varepsilon_2, \dots, \varepsilon_p) \in \mathbb{K}^p$, $\varepsilon_1 x_1 + \varepsilon_2 x_2 + \dots + \varepsilon_p x_p = 0$ et $(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_p) \neq (0,0,\dots,0)$.

Alors $(x_1, x_2, \dots, x_p)$ n'est pas libre ce qui est contraire à l'hypothèse.

Finalement $\forall (i,j) \in [\![1,p]\!]^2$, $i \neq j \Rightarrow x_i \neq x_j$.

Alors card $\{x_1, x_2, \dots, x_p\} = p$.

Or $\{x_1, x_2, \dots, x_p\} \subset \Pi_n(\mathbb{K})$. Donc $p \leq \text{card}\, \Pi_n(\mathbb{K}) \leq 2^n$.

$\forall p \in L$, $p \leq 2^n$. L est majorée. ■

L est une partie non vide et majorée de $\mathbb{N}^*$. L possède un plus grand élément r.

Alors il existe une famille $\mathbb{K}$-libre $(z_1, z_2, \dots, z_r)$ d'éléments de E.

Montrons que cette famille est une $\mathbb{K}$-base. Il ne reste plus qu'à montrer que :

$\forall x \in E, \ \exists (\varepsilon_1, \varepsilon_2, \dots, \varepsilon_r) \in \mathbb{K}^r, \ x = \varepsilon_1 z_1 + \varepsilon_2 z_2 + \dots + \varepsilon_r z_r$.

Supposons qu'il n'en soit pas ainsi. Alors il existe un élément z_{r+1} de E tel que

$z_{r+1} \notin \{ \varepsilon_1 z_1 + \varepsilon_2 z_2 + \dots + \varepsilon_r z_r \ , \ (\varepsilon_1, \varepsilon_2, \dots, \varepsilon_r) \in \mathbb{K}^r \}$.

Montrons alors que $(z_1, z_2, \dots, z_r, z_{r+1})$ est une famille $\mathbb{K}$-libre.

Soit $(\hat{\varepsilon}_1, \hat{\varepsilon}_2, \dots, \hat{\varepsilon}_{r+1}) \in \mathbb{K}^{r+1}$ tel que $\hat{\varepsilon}_1 z_1 + \hat{\varepsilon}_2 z_2 + \dots + \hat{\varepsilon}_{r+1} z_{r+1} = 0$.

1er cas. $\hat{\varepsilon}_{r+1} = 0$. Alors $\hat{\varepsilon}_1 z_1 + \hat{\varepsilon}_2 z_2 + \dots + \hat{\varepsilon}_r z_r = 0$. La liberté de $(z_1, z_2, \dots, z_r)$

donne $\hat{\varepsilon}_1 = \hat{\varepsilon}_2 = \dots = \hat{\varepsilon}_r = 0$. Ainsi $\hat{\varepsilon}_1 = \hat{\varepsilon}_2 = \dots = \hat{\varepsilon}_r = \hat{\varepsilon}_{r+1} = 0$

2ème cas $\hat{\varepsilon}_{r+1} = 1$. $z_{r+1} = 0 + z_{r+1} = (\hat{\varepsilon}_1 z_1 + \hat{\varepsilon}_2 z_2 + \dots + \hat{\varepsilon}_r z_r + z_{r+1}) + z_{r+1}$

$z_{r+1} = \hat{\varepsilon}_1 z_1 + \hat{\varepsilon}_2 z_2 + \dots + \hat{\varepsilon}_r z_r + \underbrace{(z_{r+1} + z_{r+1})}_{=0} = \hat{\varepsilon}_1 z_1 + \hat{\varepsilon}_2 z_2 + \dots + \hat{\varepsilon}_r z_r$.

Alors $z_{r+1} \in \{ \varepsilon_1 z_1 + \varepsilon_2 z_2 + \dots + \varepsilon_r z_r \ , \ (\varepsilon_1, \varepsilon_2, \dots, \varepsilon_r) \in \mathbb{K}^r \}$ ce qui est impossible par hypothèse.

Ainsi $\forall (\hat{\varepsilon}_1, \hat{\varepsilon}_2, \dots, \hat{\varepsilon}_{r+1}) \in \mathbb{K}^{r+1}, \ \hat{\varepsilon}_1 z_1 + \hat{\varepsilon}_2 z_2 + \dots + \hat{\varepsilon}_{r+1} z_{r+1} = 0 \Rightarrow \hat{\varepsilon}_1 = \hat{\varepsilon}_2 = \dots = \hat{\varepsilon}_{r+1} = 0$.

$(z_1, z_2, \dots, z_{r+1})$ est une famille $\mathbb{K}$-libre d'éléments de E de cardinal $r+1$.

Alors $r+1 \in L$. Comme r est le plus grand élément de L une légère contradiction apparaît.

Finalement $\forall x \in E, \ \exists (\varepsilon_1, \varepsilon_2, \dots, \varepsilon_r) \in \mathbb{K}^r, \ x = \varepsilon_1 x_1 + \varepsilon_2 x_2 + \dots + \varepsilon_r x_r$.

Ceci achève de montrer que $(x_1, x_2, \dots, x_r)$ est une $\mathbb{K}$-base de E.

<u>E admet une $\mathbb{K}$-base.</u>

b) • Soit $(u_1, u_2, \dots, u_p)$ une $\mathbb{K}$-base d'un code $\mathcal{C}$.

Soit $x \in \mathcal{C}$. $\exists (\varepsilon_1, \varepsilon_2, \dots, \varepsilon_p) \in \mathbb{K}^p$, $x = \varepsilon_1 u_1 + \varepsilon_2 u_2 + \dots + \varepsilon_p u_p$.

Notons l'unicité de $(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_p)$.

Soit $(\varepsilon'_1, \varepsilon'_2, \dots, \varepsilon'_p)$ un second élément de $\mathbb{K}^p$ tel que $x = \varepsilon'_1 u_1 + \varepsilon'_2 u_2 + \dots + \varepsilon'_p u_p$.

$0 = x + x = (\varepsilon_1 + \varepsilon'_1) u_1 + (\varepsilon_2 + \varepsilon'_2) u_2 + \dots + (\varepsilon_p + \varepsilon'_p) u_p$.

La liberté de $(u_1, u_2, \dots, u_p)$ donne : $\forall i \in [\![1, p]\!]$, $\varepsilon_i + \varepsilon'_i = 0$

Alors $\forall i \in [\![1, p]\!]$, $\varepsilon_i = \varepsilon_i + 0 = \varepsilon_i + \varepsilon_i + \varepsilon'_i = 0 + \varepsilon'_i = \varepsilon'_i$.

Ainsi $\forall x \in \mathcal{C}, \exists! (\varepsilon_1, \varepsilon_2, \dots, \varepsilon_p) \in \mathbb{K}^p$, $x = \varepsilon_1 u_1 + \varepsilon_2 u_2 + \dots + \varepsilon_p u_p$.

• Soit $\mathcal{C}$ un code et $(u_1, u_2, \dots, u_p)$ une $\mathbb{K}$-base de $\mathcal{C}$.

Posons $\forall (\varepsilon_1, \varepsilon_2, \dots, \varepsilon_p) \in \mathbb{K}^p$, $\varphi(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_p) = \varepsilon_1 u_1 + \varepsilon_2 u_2 + \dots + \varepsilon_p u_p$.

D'après ce qui précède φ est une application injective de $\mathbb{K}^p$ dans $\mathcal{C}$.

Comme $\mathcal{C} = \{ \varepsilon_1 u_1 + \varepsilon_2 u_2 + \dots + \varepsilon_p u_p, (\varepsilon_1, \varepsilon_2, \dots, \varepsilon_p) \in \mathbb{K}^p \}$, φ est surjective.

Alors φ est une bijection de $\mathbb{K}^p$ sur $\mathcal{C}$. Ainsi $\operatorname{card} \mathcal{C} = \operatorname{card} \mathbb{K}^p = (\operatorname{card} \mathbb{K})^p = 2^p$.

Le tout nous autorise alors à dire que :

Si un code $\mathcal{C}$ possède une base de cardinal p, $\operatorname{card} \mathcal{C} = 2^p$.

c) Soient $(u_1, u_2, \dots, u_p)$ et $(v_1, v_2, \dots, v_q)$ deux $\mathbb{K}$-bases d'un même code $\mathcal{C}$.

Alors $2^p = \operatorname{card} \mathcal{C} = 2^q$. $\quad 2^p = 2^q$. $\quad \ln 2^p = \ln 2^q$; $p \ln 2 = q \ln 2$ et

comme $\ln 2 \neq 0$ (!) $p = q$!!

Ainsi toutes les $\mathbb{K}$-bases d'un code $\mathcal{C}$ ont même cardinal.

d] Soit $(v_1, v_2, \dots, v_p)$ une famille $\mathbb{K}$-libre de $\mathcal{E}$, p étant le cardinal commun à toutes les bases de $\mathcal{E}$.

Notons que $p=r$ où r est le maximum des cardinaux des $\mathbb{K}$-familles libres de $\mathcal{E}$ d'après a]

Si $(v_1, v_2, \dots, v_p)$ n'est pas une base de $\mathcal{E}$, comme dans a] on peut trouver un élément v_{p+1} de $\mathcal{E}$ tel que $(v_1, v_2, \dots, v_p, v_{p+1})$ soit une $\mathbb{K}$-famille libre de $\mathcal{E}$.

Alors ici encore $p+1 \in L$ et $p+1 > p = r = \max L$. D'où une contradiction.

Donc nécessairement $(v_1, v_2, \dots, v_p)$ est une $\mathbb{K}$-base de $\mathcal{E}$.

Si p est le cardinal d'une $\mathbb{K}$-base de $\mathcal{E}$ et si $(v_1, v_2, \dots, v_p)$ est une $\mathbb{K}$-famille libre de $\mathcal{E}$, $(v_1, v_2, \dots, v_p)$ est une $\mathbb{K}$-base de $\mathcal{E}$.

Q4 Remarques - 1. Dans la suite si $A \in \mathcal{M}_{p,n}(\mathbb{K})$ nous noterons, pour tout $j \in [\![1, n]\!]$, $C_j(A)$ la $j^{\text{ème}}$ colonne de A.

2. Soit $A \in \mathcal{M}_{p,n}(\mathbb{K})$ et $\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \in \mathcal{M}_{n,1}(\mathbb{K})$.

$A\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \in \mathcal{M}_{p,1}(\mathbb{K})$ et surtout $A\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = x_1 C_1(A) + x_2 C_2(A) + \dots + x_n C_n(A) = \sum_{j=1}^{n} x_j C_j(A)$

a] • $0_{\mathcal{M}_{n,1}(\mathbb{K})} \in \mathcal{C}_Q$ car $Q\, 0_{\mathcal{M}_{n,1}(\mathbb{K})} = 0_{\mathcal{M}_{p,1}(\mathbb{K})}$; $\mathcal{C}_Q$ n'est pas vide.

• $\forall (x,y) \in \mathcal{C}_Q^2$, $Q(x+y) = Qx + Qy = 0 + 0 = 0$; $\forall (x,y) \in \mathcal{C}_Q$, $x+y \in \mathcal{C}_Q$.

Ainsi $\mathcal{C}_Q$ est un code.

b] L'idée est simple. Elle consiste à prendre la matrice Q et à amener par permutation des colonnes, donc de leurs indices, "les" p colonnes de Q égales à celles de I_p aux p premières places et ceci dans l'ordre.

La réalisation est un peu plus délicate

Pour tout k dans $[\![1,p]\!]$, notons j_k un élément de $[\![1,n]\!]$ tel que la $j_k^{\text{ième}}$ colonne de Q soit la $k^{\text{ième}}$ colonne de I_p.

Posons alors $\forall \ell \in [\![1,p]\!]$, $\varphi(\ell)=j_\ell$. φ est une bijection de $[\![1,p]\!]$ sur $\{j_1,j_2,\dots,j_p\}$.

ce qui peut constituer un petit abus si $p=n$ ...

$[\![p+1,n]\!]$ et $[\![1,n]\!]-\{j_1,j_2,\dots,j_p\}$ ont même cardinal donc sont équipotents.

Il existe alors une bijection ψ de $[\![p+1,n]\!]$ sur $[\![1,n]\!]-\{j_1,j_2,\dots,j_p\}$.

Posons alors $\forall \ell\in[\![1,n]\!]$, $\sigma(\ell)=\begin{cases}\varphi(\ell) & \text{si } \ell\in[\![1,p]\!]\\ \psi(\ell) & \text{sinon}\end{cases}$. Si $p=n$: $\sigma=\varphi$!

σ est clairement une bijection de $[\![1,n]\!]$ sur $[\![1,n]\!]$ donc une permutation de $[\![1,n]\!]$.

Notons que les colonnes de I_p sont dans l'ordre $C_{\sigma(1)}(Q), C_{\sigma(2)}(Q),\dots,C_{\sigma(p)}(Q)$.

Soit alors P la matrice de $M_{p,n-p}(K)$ dont les colonnes sont dans l'ordre :

$C_{\sigma(p+1)}(Q), C_{\sigma(p+2)}(Q),\dots,C_{\sigma(n)}(Q)$.

Considérons la matrice T de $M_{p,n}(K)$ dont les colonnes sont dans l'ordre $C_{\sigma(1)}(Q),\dots,C_{\sigma(n)}(Q)$.

Alors $T=(\,I_p\;\;P\,)$. Notons que si $Q=(q_{ij})$: $T=(q_{i\sigma(j)})$.

Considérons un élément $\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}$ de $M_{n,1}(K)$

$$Q\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}=\sum_{j=1}^{n} x_j\,C_j(Q)\underset{\substack{\uparrow\\ \sigma\text{ est une bijection de }[\![1,n]\!]\text{ sur }[\![1,n]\!]}}{=}\sum_{j=1}^{n} x_{\sigma(j)}\,C_{\sigma(j)}(Q)=\sum_{j=1}^{n} x_{\sigma(j)}\,C_j(T)=T\begin{pmatrix}x_{\sigma(1)}\\ \vdots\\ x_{\sigma(n)}\end{pmatrix}.$$

Ainsi $Q\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}=(\,I_p\;\;P\,)\begin{pmatrix}x_{\sigma(1)}\\ \vdots\\ x_{\sigma(n)}\end{pmatrix}$.

- Finalement il existe une matrice P de $M_{p,n-p}(K)$ et une permutation σ de $[\![1,n]\!]$ telle que : $\forall \begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}\in M_{n,1}(K)$, $Q\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}=(\,I_p\;\;P\,)\begin{pmatrix}x_{\sigma(1)}\\ \vdots\\ x_{\sigma(n)}\end{pmatrix}$ ... au moins pour $p<n$.

- Si $p=n$, il existe une permutation σ de $[\![1,n]\!]$ telle que $\forall \begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}\in M_{n,1}(K)$, $Q\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}=I_p\begin{pmatrix}x_{\sigma(1)}\\ \vdots\\ x_{\sigma(n)}\end{pmatrix}$.

c) Supposons d'abord $p<n$.

Reprenons les notations précédentes. Posons $Q=(q_{ij})$ et $T=(t_{ij})$.

$$\left.\begin{array}{l}\forall i\in[\![1,p]\!],\ \forall j\in[\![1,n]\!],\quad t_{ij}=q_{i\sigma(j)}.\\ \forall (i,j)\in[\![1,p]\!]^2,\quad t_{ij}=\begin{cases}1 \text{ si } i=j\\ 0 \text{ si } i\neq j\end{cases}\quad \text{car}\quad T=(I_p\ P).\end{array}\right\}(*)$$

Soit $x=\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}\in\mathcal{M}_{n,1}(\mathbb{K})$.

$$x\in\mathcal{C}_Q \iff Qx=0 \iff T\begin{pmatrix}x_{\sigma(1)}\\ \vdots\\ x_{\sigma(n)}\end{pmatrix}=0 \iff \forall i\in[\![1,p]\!],\ \sum_{j=1}^{n} t_{ij}\,x_{\sigma(j)}=0.$$

$x\in\mathcal{C}_Q \iff \forall i\in[\![1,p]\!]\ \ \sum_{j=1}^{p} t_{ij}\,x_{\sigma(j)}+\sum_{j=p+1}^{n} t_{ij}\,x_{\sigma(j)}=0$. En utilisant $(*)$ il vient :

$$x\in\mathcal{C}_Q \iff \forall i\in[\![1,p]\!]\ \ x_{\sigma(i)}+\sum_{j=p+1}^{n} q_{i\sigma(j)}\,x_{\sigma(j)}=0 \iff \forall i\in[\![1,p]\!],\ x_{\sigma(i)}=-\sum_{j=p+1}^{n} q_{i\sigma(j)}\,x_{\sigma(j)}.$$

un élément $x=\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}$ de $\mathcal{C}_Q$ est entièrement déterminé par la donnée de $x_{\sigma(p+1)}, x_{\sigma(p+2)}, \dots, x_{\sigma(n)}$.

$\mathcal{C}_Q$ est donc en correspondance bijective avec $\mathbb{K}^{n-p}$... montrons le.

$\forall x=\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}\in\mathcal{C}_Q$, posons $\ell(x)=(x_{\sigma(p+1)},\dots,x_{\sigma(n)})$. ℓ est une application de $\mathcal{C}_Q$ dans $\mathbb{K}^{n-p}$. Montrons qu'elle est bijective.

→ Soit $x=\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}\in\mathcal{C}_Q$ et soit $y=\begin{pmatrix}y_1\\ \vdots\\ y_n\end{pmatrix}\in\mathcal{C}_Q$ tels que $\ell(x)=\ell(y)$.

Alors $\forall i\in[\![p+1,n]\!]$, $x_{\sigma(i)}=y_{\sigma(i)}$ par définition de ℓ. Utilisons alors le fait que $x\in\mathcal{C}_Q$ et $y\in\mathcal{C}_Q$.

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

Alors $\forall i\in[\![1,n]\!]$, $x_{\sigma(i)}=y_{\sigma(i)}$. Comme σ est une bijection de $[\![1,n]\!]$ sur $[\![1,n]\!]$, $\forall i\in[\![1,n]\!]$, $x_i=y_i$. Alors $x=y$. Ceci achève de montrer que ℓ est injective.

→ Montrons que ℓ est surjective. Soit $(\alpha_1,\alpha_2,\dots,\alpha_{n-p})\in\mathbb{K}^{n-p}$.

Posons $\forall i\in[\![p+1,n]\!]$, $x_{\sigma(i)}=\alpha_{i-p}$ et $\forall i\in[\![1,p]\!]$, $x_{\sigma(i)}=-\sum_{j=p+1}^{n} q_{i\sigma(j)}\,x_{\sigma(j)}$.

Alors $x\in\mathcal{C}_Q$ et $\ell(x)=(x_{\sigma(p+1)},\dots,x_{\sigma(n)})=(\alpha_1,\dots,\alpha_{n-p})$.

Ceci achève de montrer que ℓ est surjective.

Alors l'est bijective. Ainsi $\mathcal{C}_Q$ et $\mathbb{K}^{n-p}$ sont équipotents.

card $\mathcal{C}_Q$ = card $\mathbb{K}^{n-p} = 2^{n-p}$.

$\underline{\underline{\text{card } \mathcal{C}_Q = 2^{n-p}.}}$

Alors les $\underline{\underline{\mathbb{K}\text{-bases de } \mathcal{C}_Q \text{ ont } n-p \text{ éléments}}}$

Supposons $p = n$. Soit $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathcal{M}_{n,1}(\mathbb{K})$.

$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathcal{C}_Q \Leftrightarrow Q\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0 \Leftrightarrow \underset{\text{ou } I_n\,!}{\underset{\uparrow}{I_p}} \begin{pmatrix} x_{\sigma(1)} \\ \vdots \\ x_{\sigma(n)} \end{pmatrix} = 0 \Leftrightarrow \forall i \in [\![1,n]\!],\ x_{\sigma(i)} = 0 \Leftrightarrow \forall i \in [\![1,n]\!],\ x_i = 0$

Alors $\mathcal{C}_Q = \{0\}$. card $\mathcal{C}_Q = 1 = 2^{n-p}$!

$\underline{\underline{\text{Si } n = p \text{ on a encore card } \mathcal{C}_Q = 2^{n-p}.}}$

$\underline{\text{d) Nous supposerons ici } n > p}$. Alors les bases de $\mathcal{C}_Q$ ont $n-p$ éléments.

Posons $W = \begin{pmatrix} I_{n-p} \\ B \end{pmatrix}$ et montrons que $(C_1(W), C_2(W), \dots, C_{n-p}(W))$ est une base de $\mathcal{C}_Q$

D'après Q3 d) il suffit de prouver que c'est une $\mathbb{K}$-famille libre d'éléments de $\mathcal{C}_Q$.

Montrons d'abord la liberté. Soit $(\varepsilon_1, \dots, \varepsilon_{n-p}) \in \mathbb{K}^{n-p}$ tel que $\sum_{j=1}^{n-p} \varepsilon_j C_j(W) = 0$

comme $W = \begin{pmatrix} I_{n-p} \\ B \end{pmatrix}$, pour tout $i \in [\![1, n-p]\!]$ le coefficient de la $i^{\text{ème}}$ ligne de

la matrice colonne $\sum_{j=1}^{n-p} \varepsilon_j C_j(W)$ est ε_i. Ainsi $\forall i \in [\![1, n-p]\!]$, $\varepsilon_i = 0$.

$(C_1(W), C_2(W), \dots, C_{n-p}(W))$ est une famille $\mathbb{K}$-libre.

Soit $j \in [\![1, n-p]\!]$. Montrons que $C_j(W) \in \mathcal{C}_Q$ c'est-à-dire que

$(B\ I_p)\, C_j(W) = 0$.

Posons $B = (b_{ij})$. Alors $C_j(W) = \begin{array}{c} \left.\begin{pmatrix} 0 \\ \vdots \\ 1 \\ 0 \\ \vdots \\ 0 \\ b_{1j} \\ \vdots \\ b_{pj} \end{pmatrix}\right. \end{array} \begin{array}{l} \leftarrow j^{\text{ème}} \text{ ligne} \\ \left.\right\} n-p \text{ lignes} \\ \left.\right\} p \text{ lignes} \end{array}$

1 sur la $j^{\text{ième}}$ ligne.

$$\varphi\, C_j(W) = (B\ \ I_p)\, C_j(W) = \begin{pmatrix} b_{11} & \cdots & b_{1\,n-p} & 1 & & (0) \\ \vdots & & \vdots & & \ddots & \\ b_{p1} & \cdots & b_{p\,n-p} & (0) & & 1 \end{pmatrix} \begin{pmatrix} 0 \\ \vdots \\ 1 \\ 0 \\ \vdots \\ 0 \\ b_{1j} \\ \vdots \\ b_{pj} \end{pmatrix} = \begin{pmatrix} b_{1j}+b_{1j} \\ b_{2j}+b_{2j} \\ \vdots \\ b_{pj}+b_{pj} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = 0$$

$\varphi\, C_j(W) = 0$; $C_j(W) \in \mathcal{C}_\varphi$ et ceci pour tout j appartenant à $[\![1, n-p]\!]$.

ceci achève alors de montrer que <u>les colonnes de $\begin{pmatrix} I_{n-p} \\ B \end{pmatrix}$ constituent une K-base de $\mathcal{C}_\varphi$.</u>

<u>Remarque</u>.. A titre d'exercice on pourra calculer $\varphi\, C_j(W)$ sans utiliser la juxtaposition des tableaux (première ligne ⊙) mais en utilisant la définition du produit matriciel.

On peut également remarquer, à l'aide d'un produit par blocs, que :

$(B\ \ I_p)\begin{pmatrix} I_{n-p} \\ B \end{pmatrix} = (B + B) = 0$. Cela dit alors que $\forall j \in [\![1, n-p]\!]$, $(B\ \ I_p)\, C_j(W) = 0$

e) Posons $\mathcal{S} = \{ d(x,0),\ x \in \mathcal{C}_\varphi \setminus \{0\} \}$. Notons que $\mathcal{S} \subset [\![1, n]\!]$.

<u>Etape 1</u>.. Notons que $\mathcal{S}$ n'est pas vide. Il suffit de prouver que $\mathcal{C}_\varphi \setminus \{0\} \neq \emptyset$.
Par hypothèse il existe r éléments distincts $j_1, j_2, \dots, j_r$ tels que la famille $(C_{j_1}(\varphi), \dots, C_{j_r}(\varphi))$ soit K-liée.

Ainsi $\exists (\varepsilon_{j_1}, \dots, \varepsilon_{j_r}) \in \mathbb{K}^r$, $\displaystyle\sum_{\ell=1}^{r} \varepsilon_{j_\ell}\, C_{j_\ell}(\varphi) = 0$ et $(\varepsilon_{j_1}, \dots, \varepsilon_{j_r}) \neq (0, \dots, 0)$.

Posons $\forall \ell \in [\![1, r]\!]$, $\hat{x}_{j_\ell} = \varepsilon_{j_\ell}$ et $\forall j \in [\![1, n]\!] - \{j_1, \dots, j_r\}$, $\hat{x}_j = 0$. Posons $\hat{x} = \begin{pmatrix} \hat{x}_1 \\ \vdots \\ \hat{x}_n \end{pmatrix}$.

$$\varphi\hat{x} = \sum_{j=1}^{n} \hat{x}_j\, C_j(\varphi) = \sum_{\ell=1}^{r} \hat{x}_{j_\ell}\, C_{j_\ell}(\varphi) = \sum_{\ell=1}^{r} \varepsilon_{j_\ell}\, C_{j_\ell}(\varphi) = 0$$

Alors $\hat{x} \in \mathcal{C}_\varphi$ et $\hat{x} \neq 0$ (car $(\varepsilon_{j_1}, \dots, \varepsilon_{j_r}) \neq (0, \dots, 0)$). Ainsi $\mathcal{C}_\varphi \setminus \{0\}$ n'est pas vide.

Alors $\mathcal{S} = \{ d(x, 0),\ x \in \mathcal{C}_\varphi \setminus \{0\} \}$ est une partie non vide de $[\![1, n]\!]$ (*)

(*) Rappelons que si $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, $d(x, 0) = \mathrm{card}\, \{ i \in [\![1, n]\!] \mid x_i \neq 0 \}$

$\mathcal{S}$ possède donc un plus petit élément. Montrons qu'il vaut r.

Pour cela il suffit de montrer que $r \in \mathcal{S}$ et que $\forall q \in \mathcal{S}$, $q \geq r$.

Etape 2.. Une petite remarque !

Observons l'élément $\hat{x}$ de $\mathcal{C}_Q \setminus \{0\}$ construit dans l'étape 1.

$d(\hat{x},0) = \mathrm{Card}\,\{i \in [\![1,n]\!] \mid \hat{x}_i \neq 0\} = \mathrm{Card}\,\{\ell \in [\![1,r]\!] \mid \varepsilon_{j_\ell} \neq 0\} \leq r$.

$d(\hat{x},0) \leq r$ et $\hat{x} \in \mathcal{C}_Q \setminus \{0\}$.

Etape 3.. Montrons que $\forall q \in \mathcal{S}, q \geq r$. Soit q un élément de $\mathcal{S}$.

$\exists x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathcal{C}_Q \setminus \{0\}$, $d(x,0) = q$.

$\{i \in [\![1,n]\!] \mid x_i \neq 0\}$ est un ensemble ayant q éléments que nous notons $i_1, i_2, \dots, i_q$. Notons que $x_{i_1} = x_{i_2} = \dots = x_{i_q} = 1$.

$x \in \mathcal{C}_Q$ donc $\sum_{i=1}^{n} x_i C_i(Q) = 0$. Alors $\sum_{\ell=1}^{q} x_{i_\ell} C_{i_\ell}(Q) = 0$ ou $\sum_{\ell=1}^{q} C_{i_\ell}(Q) = 0$

Par conséquent $(C_{i_1}(Q), C_{i_2}(Q), \dots, C_{i_q}(Q))$ est une famille liée de colonnes de Q.

Supposons $q < r$. Alors $q \leq r-1$ en ajoutant (éventuellement) $r-1-q$ colonnes de Q (choisies parmi les autres colonnes de Q) à cette famille nous obtenons une famille de $r-1$ colonnes de Q qui est nécessairement liée (comme sur-famille d'une famille liée). Ceci contredit l'hypothèse.

Ainsi $q \geq r$. <u>r est un minorant de $\mathcal{S}$.</u>

Etape 4.. Reprenons l'étape 2. Posons $\alpha = d(\hat{x},0)$. Nous avons $\alpha \leq r$ par construction et $\alpha \in \mathcal{S}$. Alors $\alpha \leq r$ et $\alpha \geq r$.

Donc $\alpha = r$. $r \in \mathcal{S}$.

Conclusion.. r est le plus petit élément de $\mathcal{S}$. Ainsi $r = \min\{d(x,0), x \in \mathcal{C}_Q \setminus \{0\}\}$

PARTIE III Un code correcteurs d'erreurs

(Q1) Il est aisé de montrer que $(2^\ell - \ell)_{\ell \geq 1}$ est une suite strictement croissante d'entiers.
Alors $2^p - p \geq 2^2 - 2 \geq 2$; $2^p - 1 - p \geq 1$; $n - p \geq 1$. $n > p$.

Comme $\mathbb{K}$ contient 2 éléments, $\mathcal{M}_{p,1}(\mathbb{K})$ contient 2^p éléments ; on peut donc parler de $n = 2^p - 1$ éléments non nuls de $\mathcal{M}_{p,1}(\mathbb{K})$.

Parmi ces n éléments non nuls de $\mathcal{M}_{p,1}(\mathbb{K})$ figurent les p colonnes de I_p.
Alors $H \in \mathcal{M}_{p,n}(\mathbb{K})$ et p colonnes de H sont égales aux p colonnes distinctes de I_p.
En utilisant II Q4 on peut dire que :
<u>le cardinal des $\mathbb{K}$-bases de $\mathcal{C}_H$ est $n-p$ et card $\mathcal{C}_H = 2^{n-p}$.</u>

(Q2) Nous allons nous ramener à Q4 e).
Posons $\mathcal{S}' = \{d(u,v),\ (u,v) \in \mathcal{C}_H^2 \text{ et } u \neq v\}$ et montrons que $\mathcal{S}' = \mathcal{S}$ avec $\mathcal{S} = \{d(x,0),\ x \in \mathcal{C}_H - \{0\}\}$.

- Soit $q \in \mathcal{S}'$. $\exists (u,v) \in \mathcal{C}_H^2$, $u \neq v$ et $q = d(u,v)$. Posons $x = u+v$.
  $x \in \mathcal{C}_H$ et $x \neq 0$ $(x = 0 \Rightarrow u+v = 0 \Rightarrow u+v+v = v \Rightarrow u = v\ !)$.
  Alors $x \in \mathcal{C}_H - \{0\}$ et $q = d(u,v) = d(u+v, 0) = d(x,0)$ donc $q \in \mathcal{S}$.
- Réciproquement soit $q \in \mathcal{S}$. $\exists x \in \mathcal{C}_H - \{0\}$, $q = d(x,0)$.
  Posons $u = x$ et $v = 0$. $(u,v) \in \mathcal{C}_H$, $u \neq v$ et $q = d(u,v)$! $q \in \mathcal{S}'$

Montrons alors que $\min \mathcal{S} = 3$. D'après II Q4 e il suffit de montrer qu'une famille formée de $3-1 = 2$ colonnes de H est une famille $\mathbb{K}$-libre de $\mathcal{M}_{p,1}(\mathbb{K})$ et qu'il existe une famille $\mathbb{K}$-liée formée de 3 colonnes de H.

→ Soit $C_i(H)$ et $C_j(H)$ deux colonnes distinctes de H $((i,j) \in [\![1,n]\!]^2$ et $i \neq j)$.
Montrons que $(C_i(H), C_j(H))$ est libre. Par définition de H, $C_i(H) \neq C_j(H)$.

Soit $(\alpha,\beta)\in \mathbb{K}^2$ tel que $\alpha C_i(H)+\beta C_j(H)=0$.

Supposons $\alpha\neq 0$. Alors $\alpha=1$. $C_i(H)+\beta C_j(H)=0$.

En ajoutant $C_i(H)$ de chaque côté il vient $\beta C_j(H)=C_i(H)$.

ou $\beta=0$ et $C_i(H)=0$! ou $\beta=1$ et $C_j(H)=C_i(H)$!!

Donc $\alpha=0$. Alors $\beta C_j(H)=0$. Si $\beta\neq 0$: $\beta=1$ et $C_j(H)=0$!

Ainsi $\alpha=\beta=0$.

$(C_i(H),C_j(H))$ est libre.

→ $C_1(H)+C_2(H)\in \mathcal{M}_{p,1}(\mathbb{K})$.

$C_1(H)+C_2(H)=0 \Rightarrow C_1(H)+C_2(H)+C_2(H)=C_2(H) \Rightarrow C_1(H)=C_2(H)$!

Donc $C_1(H)+C_2(H)$ est un élément non nul de $\mathcal{M}_{p,1}(\mathbb{K})$ donc une colonne de H.

$\exists i\in [\![1,n]\!]$, $C_1(H)+C_2(H)=C_i(H)$.

$i=1 \Rightarrow C_1(H)+C_2(H)=C_1(H)\Rightarrow C_2(H)=0$!

$i=2 \Rightarrow C_1(H)+C_2(H)=C_2(H)\Rightarrow C_1(H)=0$!

Alors $C_1(H)$, $C_2(H)$ et $C_i(H)$ sont trois colonnes distinctes de H.

$C_1(H)+C_2(H)+C_i(H)=C_i(H)+C_i(H)=0$

$(C_1(H),C_2(H),C_i(H))$ est une famille $\mathbb{K}$-liée constituée de trois colonnes distinctes de H.

Ceci achève de prouver que $\min \mathcal{S}=3$. Alors $\min \mathcal{S}'=3$.

$\min\{d(u,v),(u,v)\in \mathcal{C}_H^2 \text{ et } u\neq v\}=3$.

Q3) a) Soit $v\in\mathcal{M}_{n,1}(\mathbb{K})$. v a n composantes qui sont des éléments de $\mathbb{K}$ et $\mathbb{K}$ a deux éléments.

Fixons i dans $[\![1,n]\!]$

Il y a un élément de $\mathcal{M}_{n,1}(\mathbb{K})$ qui diffère de v par sa seule $i^{\text{ème}}$ composante.

Il y a donc exactement n éléments de $\mathcal{M}_{n,1}(\mathbb{K})$ dont toutes les composantes coïncident avec celles de v sauf une qui est différente.

Alors $\{u\in \mathcal{M}_{n,1}(\mathbb{K})\mid d(u,v)=1\}$ a pour cardinal n.

Alors $B_v = \{u \in \mathcal{M}_{n,1}(\mathbb{K}) \mid d(u,v) \leq 1\}$ a $n+1$ éléments ($d(u,v)=0 \Leftrightarrow u=v$).

$\operatorname{card} B_v = n+1 = 2^p$.

b) Soit $(v,w) \in \mathcal{C}_H^2$ et $v \neq w$. Montrons que $B_v \cap B_w = \emptyset$

Supposons qu'il existe $u \in B(v) \cap B(w)$.

$d(v,w) \leq d(v,u) + d(u,w) \leq 2$.

$(v,w) \in \mathcal{C}_H^2$, $v \neq w$ et $d(v,w) \leq 2$. Ceci contredit le résultat de Q2.

Ainsi $\forall (v,w) \in \mathcal{C}_H^2$, $v \neq w \Rightarrow B_v \cap B_w = \emptyset$.

c) Rappelons que $\mathcal{M}_{n,1}(\mathbb{K})$ est un ensemble fini ayant 2^n éléments et que $\bigcup_{v \in \mathcal{C}_H} B_v \subset \mathcal{M}_{n,1}(\mathbb{K})$.

Pour montrer $\bigcup_{v \in \mathcal{C}_H} B_v = \mathcal{M}_{n,1}(\mathbb{K})$ il suffit alors de montrer que $\operatorname{card} \bigcup_{v \in \mathcal{C}_H} B_v = 2^n$

D'après b) $\operatorname{card} \bigcup_{v \in \mathcal{C}_H} B_v \overset{\text{"union disjointe"}}{=} \sum_{v \in \mathcal{C}_H} \operatorname{card} B_v$.

a) donne alors $\operatorname{card} \bigcup_{v \in \mathcal{C}_H} B_v = \sum_{v \in \mathcal{C}_H} 2^p = 2^p \times \operatorname{card} \mathcal{C}_H = 2^p \times 2^{n-p} = 2^n$.

Ceci achève de montrer que $\mathcal{M}_{n,1}(\mathbb{K}) = \bigcup_{v \in \mathcal{C}_H} B_v$.

Q4 a) $z \in \mathcal{M}_{n,1}(\mathbb{K}) \setminus \mathcal{C}_H$. $z \notin \mathcal{C}_H$ et $z \in \bigcup_{v \in \mathcal{C}_H} B_v$ car $\bigcup_{v \in \mathcal{C}_H} B_v = \mathcal{M}_{n,1}(\mathbb{K})$

Alors $\exists v \in \mathcal{C}_H$, $z \in B_v$. Ainsi $d(z,v) \leq 1$.

Si $d(z,v) = 0$ alors $z = v$ et $z \in \mathcal{C}_H$!

Donc $v \in \mathcal{C}_H$ et $d(z,v) = 1$. Supposons qu'il existe v' dans $\mathcal{C}_H$ distinct de v tel que $d(z,v') = 1$.

Alors $(v,v') \in \mathcal{C}_H^2$, $v \neq v'$ et $d(v,v') \leq d(v,z) + d(z,v') \leq 2$. Ceci est impossible.

$\exists !\, v \in \mathcal{C}_H,\ d(z, v) = 1.$

b) Soit e un élément de $\mathcal{M}_{n,1}(\mathbb{K})$.

$Hz = He \iff Hz + He = He + He \iff H(z+e) = 0 \iff z+e \in \mathcal{C}_H.$

Rappelons que $d(z, z+e) = d(z+z+e, 0) = d(e, 0)$.

Alors $\begin{cases} d(e,0)=1 \\ \text{et} \\ Hz = He \end{cases} \iff \begin{cases} z+e \in \mathcal{C}_H \\ \text{et} \\ d(z, z+e) = 1 \end{cases} \iff \phi(z) = z+e \iff \phi(z) + z = e.$

Ainsi $\exists !\, e \in \mathcal{M}_{n,1}(\mathbb{K}),\ d(e,0) = 1$ et $Hz = He$.

$e = \phi(z) + z$ et $e + z = \phi(z)$.

QS a) $H_1 = (B \ \ I_3)$ avec $B = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$. $\left| \begin{array}{l} p = 3 \\ n = 2^3 - 1 = 7 \end{array} \right.$ $|\ n - p = 4$

D'après II Q4 d) les colonnes de $\begin{pmatrix} I_{7-3} \\ B \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$ constituent une base de $\mathcal{C}_{H_1}$

Alors $(c_1, c_2, c_3, c_4) = \left(\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \end{pmatrix} \right)$ est une $\mathbb{K}$-base de $\mathcal{C}_{H_1}$.

b) $H_1 y^* = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1+1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}.$

Ainsi $H_1 y^* \neq 0$ donc $y^* \in \mathcal{M}_{7,1}(\mathbb{K}) \setminus \mathcal{C}_H$.

Or $y \in \mathcal{C}_H$ et $d(y, y^*) = 1$. Ainsi $y = \phi(y^*)$

$y = \phi(y^*) = y^* + e$ où e est l'élément de $\mathcal{M}_{7,1}(\mathbb{K})$ tel que

$d(e, 0) = 1$ et $H_1 y^* = H_1 e$

Il reste plus pour obtenir y qu'à trouver l'élément e de $\mathcal{M}_{7,1}(\mathbb{K})$

dont toutes les composantes sont nulles, sauf une qui est égale à 1 et qui vérifie $H_1 e = H_1 y^* = \begin{pmatrix}1\\0\\1\end{pmatrix}$.

Comme $\begin{pmatrix}1\\0\\1\end{pmatrix}$ est la troisième colonne de H_1 : $e = \begin{pmatrix}0\\0\\1\\0\\0\\0\\0\end{pmatrix}$.

C'est la troisième composante de y^* qui est fausse.

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

Observons que $y = c_2 + c_3$. Alors $n_1 = 0$, $n_2 = 1$, $n_3 = 1$ et $n_4 = 0$.

c) Nécessairement $H_1 z^* \neq 0$. En effet si $H_1 z^* = 0$ alors $(z, z^*) \in \mathcal{C}_H^2$ et $d(z, z^*) = 2$ ce qui est impossible.

Si l'on sait qu'il y a au plus deux erreurs un $H_1 z^* \neq 0$ indique qu'il y eu un problème dans la transmission.

Remarque. Ce n'est pas le cas si il y a eu au moins trois erreurs.

Supposons que deux composantes exactement sont fausses.

$z = z^* + e$ avec $d(e, 0) = 2$ et $H z^* = He$.

Il y a $\binom{7}{2}$, c'est à dire 21, éléments e de $\mathcal{M}_{7,1}(\mathbb{K})$ qui vérifient $d(e, 0) = 2$

or $\{He \ ; \ e \in \mathcal{M}_{7,1}(\mathbb{K})$ et $d(e, 0) = 2\} \subset \mathcal{M}_{3,1}(\mathbb{K})$. Sachant que $\mathcal{M}_{3,1}(\mathbb{K})$ a $2^3 = 8$ éléments il peut exister plusieurs éléments e de $\mathcal{M}_{7,1}(\mathbb{K})$ tels que $d(e, 0) = 2$ et $H z^* = He$. On ne peut donc pas toujours déduire z de z^*.

Ainsi on ne peut pas toujours connaître les deux composantes qui sont fausses.

PARTIE IV Distinguere falsum vero

(Q1) Avant de répondre à la question éclairons le propos.

Nous avons vu que H est construite des éléments non nuls de $\mathcal{M}_{p,1}(\mathbb{K})$.
Comme nous l'a montré la question 5 il est important de situer un élément non nul de $\mathcal{M}_{p,1}(\mathbb{K})$ dans H (à partir de $H_1 y^*$ il faut savoir trouver $e \in \mathcal{M}_{p,1}(\mathbb{K})$ tel que $H_1 y^* = H_1 e$ et $d(e,0)=1 \dots$). Plus précisément, si t est un élément de $\mathcal{M}_{p,1}(\mathbb{K}) - \{0\}$, il faut savoir trouver k dans $[\![1,n]\!]$ tel que $t = C_k(H)$.

Si la matrice H est construite de manière quelconque la tâche est impossible.
On nous propose une construction logique de H, basée sur l'écriture d'un entier en base 2, qui rend le travail simple pour nous et pour la machine.

Soit $t = \begin{pmatrix} t_1 \\ \vdots \\ t_p \end{pmatrix}$ un élément non nul de $\mathcal{M}_{p,1}(\mathbb{K})$; $\forall i \in [\![1,p]\!]$, $t_i = 0$ ou 1 et $(t_1, t_2, \dots, t_p) \neq 0_{\mathbb{K}^p}$.

Associons à $t = \begin{pmatrix} t_1 \\ \vdots \\ t_p \end{pmatrix}$ l'entier N_t qui s'écrit $\overline{t_p t_{p-1} \dots t_1}^{2}$ en base 2.

Notons que $N_t = \sum_{i=1}^{p} 2^{i-1} t_i$ et que $N_t \in [\![1, 2^p - 1]\!] = [\![1, n]\!]$

Il est aisé de montrer que l'application $\mathcal{L}$ de $\mathcal{M}_{p,1}(\mathbb{K}) - \{0\}$ dans $[\![1,n]\!]$, qui à $t = \begin{pmatrix} t_1 \\ \vdots \\ t_p \end{pmatrix}$ associe $N_t = \overline{t_p t_{p-1} \dots t_1}^{2} = \sum_{i=1}^{p} 2^{i-1} t_i$ est une bijection. $\underline{\mathcal{L}}$ numérote les éléments de $\mathcal{M}_{p,1}(\mathbb{K}) - \{0\}$!

Alors $\mathcal{L}^{-1}$ est une bijection de $[\![1,n]\!]$ dans $\mathcal{M}_{p,1}(\mathbb{K}) - \{0\}$.

Alors nous prendrons pour matrice H la matrice H_2 telle que, pour tout $k \in [\![1,n]\!]$, la $k^{\text{ième}}$ colonne de H_2 soit $\mathcal{L}^{-1}(k)$.

Pratiquement si k est élément de $[\![1,n]\!] = [\![1, 2^p - 1]\!]$, pour obtenir la $k^{\text{ième}}$ colonne de H_2 on écrit k en base deux à $\underline{p \text{ positions}}$. Ceci donne $k = \overline{t_p t_{p-1} \dots t_1}^{2}$. Ainsi $C_k(H_2) = \begin{pmatrix} t_1 \\ \vdots \\ t_p \end{pmatrix}$.

<u>Exerçons-nous</u> avec $p=3$ et donc $n = 2^3-1 = 7$.

1, 2, 3, 4, 5, 6, 7 s'écrivent respectivement en base 2 à trois positions :

001, 010, 011, 100, 101, 110, 111.

Ainsi $H_2 = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$.

Il est temps de répondre à la question !

On suppose que $H_2 y^* = \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix}$. Posons $k = \sum_{i=1}^{p} x_i 2^{i-1}$; alors $H_2 y^*$ est la $k^{\text{ième}}$ colonne de H_2. Posons $e_k = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \leftarrow k^{\text{ième}}$ ligne.

$H_2 y^* = H_2 e_k$ et $d(e_k, 0) = 1$.

Ainsi $y = \phi(y^*) = y^* + e_k$. <u>L'erreur s'est produite à la composante numéro k de y.</u>

(Q2) <u>a)</u> Nous avons vu plus haut que $H_2 = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$

Les colonnes reçues sont $c_1^* = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}$, $c_2^* = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}$, $c_3^* = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}$. Notons c_1, c_2, c_3 les colonnes transmises.

Un calcul simple donne $H_2 c_1^* = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$. $\overline{011}^2 = 3$. $H_2 c_1^*$ est la troisième colonne de H_2. $H_2 c_1^* = H_2 e_3$ où $e_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$. $d(e_3, 0) = 1$ donc

$c_1 = \phi(c_1^*) = c_1^* + e_3 = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}$. La troisième composante de c_1 a été mal transmise...

Montrons alors que (d_1, d_2, d_3, d_4) est une base de $\mathcal{C}_{H_2}$.

Des calculs simples donnent $H_2 d_i = 0$ pour tout i dans $[\![1,4]\!]$.

(d_1, d_2, d_3, d_4) est une famille de $\mathcal{C}_{H_2}$. Montrons que cette famille est libre.

Soit $(\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4) \in \mathbb{K}^4$ tel que $\varepsilon_1 d_1 + \varepsilon_2 d_2 + \varepsilon_3 d_3 + \varepsilon_4 d_4 = 0$.

Alors $\begin{pmatrix} \varepsilon_1 \\ \varepsilon_2 \\ \varepsilon_3 \\ \varepsilon_4 \\ \varepsilon_2+\varepsilon_3+\varepsilon_4 \\ \varepsilon_1+\varepsilon_3+\varepsilon_4 \\ \varepsilon_1+\varepsilon_2+\varepsilon_4 \end{pmatrix} = 0$. Ainsi $\varepsilon_1 = \varepsilon_2 = \varepsilon_3 = \varepsilon_4 = 0$.

(d_1, d_2, d_3, d_4) est une famille $\mathbb{K}$-libre de quatre éléments de $\mathcal{C}_{H_2}$ et les $\mathbb{K}$-bases de $\mathcal{C}_{H_2}$ ont $n-p = 7-3 = 4$ éléments. Alors d'après II Q3 d], (d_1, d_2, d_3, d_4) est une $\mathbb{K}$-base de $\mathcal{C}_{H_2}$.

Notons que si $u = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_7 \end{pmatrix}$ est un élément de $\mathcal{C}_{H_2}$, ses coordonnées dans la $\mathbb{K}$-base (d_1, d_2, d_3, d_4) sont : (u_1, u_2, u_3, u_4).

Ainsi $c_1 = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = d_1 + d_2 + 0\, d_3 + 0\, d_4$. Alors $x_1 = 1, x_2 = 1, x_3 = 0, x_4 = 0$.

Ainsi $x = \overline{0011}^2$. $x = 3$.

$H_2 c_2^* = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$. Alors $c_2 = c_2^*$. Il n'y a pas eu d'erreur.

$c_2 = c_2^* = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} = 1.d_1 + 0.d_2 + 0.d_3 + 0.d_4$. $y_1 = 1$, $y_2 = y_3 = y_4 = 0$. $y = 1$.

$H_2 C_3^* = \begin{pmatrix}1\\1\\1\end{pmatrix}$ $\overline{111}^2 = 7$. $H_2 C_3 = H_2 e_7$ avec $e_7 = \begin{pmatrix}0\\0\\0\\0\\0\\0\\1\end{pmatrix}$.

Donc $H_2 C_3^* = H_2 e_7$ avec $d(e_7, 0) = 1$.

$C_3 = \phi(C_3^*) = C_3 + e_7 = \begin{pmatrix}0\\0\\1\\0\\1\\1\\0\end{pmatrix} = 0.d_1 + 0.d_2 + 1.d_3 + 0.d_4$.

$\underline{\underline{z_1=0,\ z_2=0,\ z_3=1,\ z_4=0}}$ et $\underline{\underline{z = \overline{0100}^2 = 4}}$

Les trois premiers chiffres significatifs de z sont 3 1 4

$314 \simeq 100\pi$. Je vous laisse la pitoyable CONclusion.

c) Il convient avant tout d'écrire un programme qui permet à partir d'une colonne reçue, et sachant qu'il y a au plus une erreur de retrouver le chiffre transmis.

Point 0.. Quelques déclarations initiales.

```
Program hec2004M1;

uses crt;
const P_Max=8;
type matrice= array[1..8,1..255] of integer;
     colonne=array[1..255] of integer;
```

} (*)

On choisit ici de limiter p à 8. Si ce n'est pas le cas il suffit de modifier le bloc (*)

Point 1.. Construction de H_2

```
procedure construit_H2(p,n:integer;var H:matrice);

var k,j,q,l:integer;

begin


for k:=1 to n do
    begin
    q:=k;j:=0;
    repeat
    j:=j+1;H[j ,k]:=(q mod 2);q:=q div 2;
    until (q=0);
    for l:=j+1 to p do H[l,k]:=0;
    end;

end;
```

On construit H_2 en se rappelant que la colonne k de H_2 est l'"écriture" en base 2 à p positions de l'entier k. On obtient cette écriture en prenant les restes successifs dans des divisions de k par 2. On n'oublie pas de compléter la colonne par des zéros.

Point 2 .. Détermination du rang éventuel de l'erreur.

```
function rang_erreur(n,p:integer;H2:matrice;C:colonne):integer;

var i,j,k,s,puis:integer;

begin
k:=0;puis:=1;
for i:=1 to p do
    begin
    s:=0;
    for j:=1 to n do s:=s+H2[i,j]*C[j];
    if (s mod 2)=1 then k:=k+puis;
    puis:=puis+puis;
    end;
rang_erreur:=k;
end;
```

Le principe est simple. A partir de la colonne reçue $C=\begin{pmatrix}c_1\\ \vdots\\ c_n\end{pmatrix}$ on calcule $H_2C=\begin{pmatrix}t_1\\ \vdots\\ t_p\end{pmatrix}$ et l'on obtient $k=\overline{t_p\, t_{p-1}\cdots t_1}^{2}$. Le test se fait simultanément : si $\ell=0$ il n'y a pas d'erreur. Si $\ell \geq 1$ $H_2C=\begin{pmatrix}t_1\\ \vdots\\ t_p\end{pmatrix}$ n'est autre que la $\ell^{ième}$ colonne de H_2 donc $H_2C=H_2e_\ell$ avec $e_\ell=\begin{pmatrix}0\\ \vdots\\ 0\\ 1\\ 0\\ \vdots\\ 0\end{pmatrix}\leftarrow \ell^{e}$ ligne. L'erreur se situe au niveau de la $\ell^{ième}$ composante de C.

Notons que $\ell=\sum_{i=1}^{p}\left(\sum_{j=1}^{n} h_{ij}c_j\right)2^{i-1}$ (*)

Notons encore qu'il faut transformer $\sum_{j=1}^{n} h_{ij}c_j$ en un élément de $\mathbb{K}=\{0,1\}$. Si $\sum_{j=1}^{n} h_{ij}c_j$ est impair c'est le 1 de $\mathbb{K}$ sinon c'est le 0 !! Dans ce dernier cas sa participation à la somme sur i de (*) est nulle.

Notons également qu'on obtient s est impair si le reste dans la division par 2 de s est 1

Point 3 .. le programme principal.

E1 on demande p et on calcule n.

E2 on appelle la procédure construit_H2 pour obtenir H2

E3 on demande à l'utilisateur la colonne reçue

E4 détermination du rang de l'erreur éventuelle

E5 correction de l'erreur éventuelle.

E5 calcul du chiffre transmis. C'est $\sum_{i=1}^{p} c'_i\, 2^{i-1}$ où $\begin{pmatrix}c'_1\\ \vdots\\ c'_n\end{pmatrix}$ est la colonne corrigée.

```
(* Déclaration des variables du programme principal *)

var n,p,i,k,puis,nombre:integer;H:matrice;C:colonne;

begin

(* Introduction de p *)

write('Donner la valeur de p (p<=',P_max,'). p=');readln(p);

(* Calcul de n *)

puis:=1;
for i:=1 to p do puis:=puis+puis;
n:=puis-1;

(* Construction de H2 *)

construit_H2(p,n,H);

(* Introduction de la colonne reçue *)

writeln('Entrée de la colonne reçue');writeln;

for i:=1 to n do
    begin
    write('Donner c',i,'. c',i,'=');readln(C[i]);
    end;

(* Détermination du rang éventuel de l'erreur *)

k:=rang_erreur(n,p,H,C);

(* Correction de l'erreur éventuelle *)

If k=0 then writeln('il n''y a pas d''erreur')
        else begin
             writeln('L''erreur se trouve à la composante numéro ',k);
             if C[k]=1 then C[k]:=0
                       else C[k]:=1;
             end;

(* Détermination du chiffre transmis *)

puis:=1;nombre:=0;
for k:=1 to p do
    begin
    nombre:=nombre+puis*C[k];
    puis:=puis+puis;
    end;
writeln('Le nombre est : ',nombre);
end.
```

▲ Il faut évidemment prévoir la possibilité pour l'utilisateur de refaire plusieurs fois le travail sans recalculer H2.

Une petite exécution →

```
Donner la valeur de p (p<=8). p=3
Entrée de la colonne reçue

Donner c1. c1=1
Donner c2. c2=1
Donner c3. c3=1
Donner c4. c4=0
Donner c5. c5=1
Donner c6. c6=1
Donner c7. c7=0
L'erreur se trouve à la composante numéro 3
Le nombre est : 3
```

Pour faire la même chose en utilisant des booleans !

```
Program hec2004M1;

uses crt;
const P_Max=8;
type matrice= array[1..8,1..255] of boolean;
     colonne=array[1..255] of boolean;
```

```
procedure construit_H2(p,n:integer;var H:matrice);

var k,j,q,l:integer;

begin


for k:=1 to n do
    begin
    q:=k;j:=0;
    repeat
    j:=j+1;
    H[j,k]:=odd(q mod 2);
    q:=q div 2;
    until (q=0);
    for l:=j+1 to p do H[l,k]:=false;
    end;

end;
```

on peut aussi écrire H[j,l]:= (q mod 2)=1 ce qui évite l'utilisation de odd

c'est un booléen !!

```
Function mat_colo(n,i:integer;H:matrice;C:colonne):boolean;

var j:integer;s:boolean;

begin
s:=false;
For j:=1 to:n do
s:=(s xor  H[i,j] and C[j]));
mat_colo:=s;
end;
```

J'ai ajouté cette fonction qui calcule $\sum_{j=1}^{n} h_{ij} c_j$ c'est à dire la ième composante de $H \times C$ ou HC !

On est prié d'observer l'utilisation des opérations sur les boolean|booléens

```
function rang_erreur(n,p:integer;H:matrice;C:colonne):integer;

var i,j,k,s,puis:integer;

begin
k:=0;puis:=1;
for i:=1 to p do
    begin
    if mat_colo(n,i,H,C) then k:=k+puis;
    puis:=puis+puis;
    end;
rang_erreur:=k;
end;
```

```
var n,p,i,k,puis,nombre:integer;H:matrice;C:colonne;

begin

write('Donner la valeur de p (p<=',P_Max,'). p=');readln(p);

puis:=1;
```

```
for i:=1 to p do puis:=puis+puis;

n:=puis-1;

construit_H2(p,n,H);

writeln('Entrée de la colonne reçue');writeln;

for i:=1 to n do
    begin
    write('Donner c',i,'. c',i,'=');readln(nombre);
    C[i]:=(nombre=1);
    end;


writeln;

k:=rang_erreur(n,p,H,C);

If k=0 then writeln('il n''y a pas d''erreur')
        else begin
             writeln('L''erreur se trouve à la composante numéro ',k);
             C[k]:=not(C[k]);
             end;

puis:=1;nombre:=0;
for k:=1 to p do
    begin
    if C[k] then nombre:=nombre+puis;
    puis:=puis+puis;
    end;
writeln('Le nombre est : ',nombre)
end.
```

```
Donner la valeur de p (p<=8). p=3
Entrée de la colonne reçue

Donner c1. c1=1
Donner c2. c2=0
Donner c3. c3=0
Donner c4. c4=0
Donner c5. c5=0
Donner c6. c6=1
Donner c7. c7=1
il n'y a pas d'erreur
Le nombre est : 1
```

```
Donner la valeur de p (p<=8). p=3
Entrée de la colonne reçue

Donner c1. c1=0
Donner c2. c2=0
Donner c3. c3=1
Donner c4. c4=0
Donner c5. c5=1
Donner c6. c6=1
Donner c7. c7=1
L'erreur se trouve à la composante numéro 7
Le nombre est : 4
Press any key to return to Turbo Pascal
```