

DEVOIR SURVEILLÉ 3

(durée : 3 h 30)

Rédigez vos réponses dans un français correct. Terminez chaque résolution d'exercice par une conclusion encadrée ou soulignée. Laissez une marge au correcteur.

Les exercices sont indépendants et peuvent être traités dans n'importe quel ordre. Dans un exercice avec plusieurs questions, on pourra, si besoin est, admettre le résultat d'une question pour répondre aux suivantes.

La calculatrice n'est pas autorisée.

EXERCICE 1

Séquences de Skolem

Une séquence de Skolem d'ordre n est un $2n$ -uplets constitué des entiers de 1 à n répétés chacun deux fois, tel que, pour tout $k \in \llbracket 1; n \rrbracket$, les deux apparitions de l'entier k soient distantes de k .

Par exemple, $(4, 5, 1, 1, 4, 3, 5, 2, 3, 2)$ est une séquence de Skolem d'ordre 5 puisque les deux 1 sont distants d'une unité, les deux 2 sont distants de deux unités, les deux 3 sont distants de trois unités, les deux 4 sont distants de quatre unités et les deux 5 sont distants de cinq unités.

On se donne une séquence de Skolem d'ordre n (où $n \in \mathbb{N}^*$), c'est-à-dire une famille $(x_i)_{1 \leq i \leq 2n}$ d'entiers dans $\llbracket 1; n \rrbracket$ telle que, pour tout nombre $k \in \llbracket 1; n \rrbracket$, il existe exactement deux indices distincts a_k et b_k dans $\llbracket 1; 2n \rrbracket$ tels que $b_k - a_k = k$ et $x_{a_k} = x_{b_k} = k$. On notera, qu'avec ces notations, on a $a_k < b_k$ autrement dit que a_k est le premier rang où l'on rencontre k et b_k est le second.

1. Pour la séquence de Skolem $(4, 5, 1, 1, 4, 3, 5, 2, 3, 2)$, donner a_k et b_k pour $k \in \llbracket 1; 5 \rrbracket$.
2. Démontrer que

$$\sum_{k=1}^n a_k = n^2 - \frac{n(n-1)}{4}.$$

Indication : Utiliser les b_k .

3. En déduire que n ou $n - 1$ est un multiple de 4.

On a ainsi démontré qu'il ne peut exister de séquence de Skolem d'ordre n que si n est congru à 0 ou 1 modulo 4. Dans ces deux cas, on sait construire des séquences de Skolem.

EXERCICE 2

Transformée de Fourier discrète

Soit $n \in \mathbb{N}^*$. On pose $\omega = e^{2i\pi/n}$.

Si u est un n -uplet de \mathbb{C}^n , on note $u = (u_0, u_1, \dots, u_{n-1})$ ou encore $u = (u_k)_{k \in \llbracket 0; n-1 \rrbracket}$. De plus, on pose $u_{-1} = u_{n-1}$, $u_{-2} = u_{n-2}$, ..., $u_{-(n-1)} = u_1$.

Pour tous n -uplets u, v de \mathbb{C}^n , on appelle *produit de convolution discret* de u et v le n -uplet $u \otimes v = (a_0, a_1, \dots, a_{n-1})$ de \mathbb{C}^n défini par

$$\forall j \in \llbracket 0; n-1 \rrbracket, \quad a_j = \sum_{k=0}^{n-1} u_k v_{j-k}$$

On considère la *tranformée de Fourier discrète* sur \mathbb{C}^n , c'est-à-dire l'application

$$F \left\{ \begin{array}{ccc} \mathbb{C}^n & \longrightarrow & \mathbb{C}^n \\ (u_0, u_1, \dots, u_{n-1}) & \longmapsto & (b_0, b_1, \dots, b_{n-1}) \end{array} \right.$$

où

$$\forall k \in \llbracket 0; n-1 \rrbracket, \quad b_k = \sum_{j=0}^{n-1} \overline{u_j} \omega^{kj}.$$

On rappelle que $(\mathbb{C}^n, +, \times)$ est un anneau commutatif (où $+$ et \times sont respectivement l'addition et la multiplication terme à terme).

On admet que $(\mathbb{C}^n, +, \otimes)$ est également un anneau commutatif.

1. Trois questions préliminaires

a) Soit $m \in \mathbb{Z}$. Calculer

$$\sum_{j=0}^{n-1} \omega^{mj}.$$

Indication: On ne trouve pas toujours 0.

b) Soient $k, p \in \llbracket 0; n-1 \rrbracket$ et $u \in \mathbb{C}^n$. Démontrer que

$$\sum_{j=-p}^{n-1-p} \overline{u_j} \omega^{kj} = \sum_{j=0}^{n-1} \overline{u_j} \omega^{kj}.$$

c) Quel est l'élément neutre pour \otimes ?

2. Transformée de Fourier inverse

Calculer $F \circ F$.

En déduire que F est une bijection dont on précisera la réciproque.

3. Transformée de Fourier et convolution

a) Démontrer que, pour tous $u, v \in \mathbb{C}^n$, on a $F(u + v) = F(u) + F(v)$.

b) Démontrer que, pour tous $u, v \in \mathbb{C}^n$, on a $F(u \otimes v) = F(u) \times F(v)$.

c) Démontrer que F est un isomorphisme d'anneaux entre $(\mathbb{C}^n, +, \otimes)$ et $(\mathbb{C}^n, +, \times)$.

4. Équation de convolution

Soient $u, v \in \mathbb{C}^n$. Déterminer une condition nécessaire et suffisante sur $F(u)$ et $F(v)$ pour que l'équation $u \otimes x = v$ d'inconnue $x \in \mathbb{C}^n$ admette au moins une solution.

EXERCICE 3

Loto Foot 15

Au Loto Foot 15, le parieur remplit une grille dans laquelle il indique ses prévisions pour quinze matchs de football à venir. Pour chacun des matchs, il peut cocher au choix une des trois cases : pour une victoire de l'équipe qui reçoit, pour une victoire de l'équipe qui se déplace et pour un match nul. À l'issue du match, une et une seule de ces trois possibilités sera réalisée.

On donnera les résultats sous forme de sommes ou de produits d'entiers ou de coefficients binomiaux sans chercher à les calculer.

1. De combien de façons un parieur peut-il remplir la grille ?
2. Pour gagner, il faut avoir coché au moins douze réponses exactes. Quel est le nombre de grilles gagnantes ?

EXERCICE 4

Codage de Hamming

On considère un système de transmission (ligne téléphonique, fibre optique, WiFi, ...) qui émet, vers un récepteur, des messages constitués de p bits (c'est-à-dire des nombres de p chiffres pris dans $\{0; 1\}$). Lors de cette transmission, des « bruits » peuvent venir parasiter le message, ce qui conduit à l'inversion de certains bits. Sans contrôle, l'information est alors irrémédiablement altérée.

Le codage de Hamming est une méthode développée en 1950 par Richard Hamming pour transmettre des messages « contrôlés » qui permettent au récepteur de détecter la présence (voire de corriger) des erreurs de transmission.

L'objet de cet exercice est de présenter les bases théoriques de ce codage.

1. Anneau de Boole des parties d'un ensemble fini

Soit E un ensemble fini de cardinal n (où $n \in \mathbb{N}^*$). Pour A et B deux parties de E , on définit la différence symétrique de A et B , notée $A\Delta B$, par

$$A\Delta B = (A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A).$$

En exercice, nous avons démontré que, pour toutes parties A et B de E , on a :

- 1) Δ est une opération associative et commutative ;
- 2) $A\Delta A = \emptyset$ et même, plus précisément, $(A\Delta B = \emptyset) \iff (A = B)$;
- 3) \cap est distributive sur Δ .

Ces propriétés sont supposées acquises.

- a) Justifier que $(\mathcal{P}(E), \Delta, \cap)$ est un anneau commutatif. On précisera les éléments neutres et, pour tout $A \in \mathcal{P}(E)$, on donnera le symétrique de A pour la loi Δ .
- b) Déterminer $U(\mathcal{P}(E))$, c'est-à-dire le groupe des éléments inversibles de $\mathcal{P}(E)$.
L'anneau $(\mathcal{P}(E), \Delta, \cap)$ est-il un corps ?
- c) $\alpha]$ Soit $A \in \mathcal{P}(E)$. Démontrer que $\mathcal{P}(A)$ est un idéal de $\mathcal{P}(E)$.
 $\beta]$ Soit \mathcal{I} un idéal de $\mathcal{P}(E)$. Démontrer que

$$\forall X \in \mathcal{I}, \quad \forall Y \subset X, \quad Y \in \mathcal{I} \quad \text{et} \quad \forall X, Y \in \mathcal{I}, \quad X \cup Y \in \mathcal{I}.$$

En déduire l'existence de $A \in \mathcal{P}(E)$ tel que $\mathcal{I} = \mathcal{P}(A)$.

2. Distance de Hamming

Soit E un ensemble fini de cardinal n (où $n \in \mathbb{N}^*$). Pour A et B deux parties de E , on définit la distance de Hamming $d(A, B)$ entre A et B par

$$d(A, B) = \text{card}(A \Delta B).$$

- a) Démontrer que la distance de Hamming d est une métrique sur $\mathcal{P}(E)$, c'est-à-dire une application de $\mathcal{P}(E) \times \mathcal{P}(E)$ vers \mathbb{R} telle que :
- (i) $\forall A, B \in \mathcal{P}(E), d(A, B) \geq 0$ (positivité) ;
 - (ii) $\forall A, B \in \mathcal{P}(E), d(A, B) = d(B, A)$ (symétrie) ;
 - (iii) $\forall A, B \in \mathcal{P}(E), (d(A, B) = 0) \iff (A = B)$ (séparation) ;
 - (iv) $\forall A, B, C \in \mathcal{P}(E), d(A, C) \leq d(A, B) + d(B, C)$ (inégalité triangulaire).

On dit alors que le couple $(\mathcal{P}(E), d)$ est un espace métrique.

- b) Soient $\Omega \in \mathcal{P}(E)$ et $r \in \mathbb{N}$. Dans l'espace métrique $(\mathcal{P}(E), d)$, on définit la sphère $\mathcal{S}(\Omega, r)$ de centre Ω et de rayon r ainsi que la boule $\mathcal{B}(\Omega, r)$ de centre Ω et de rayon r de la façon suivante :

$$\mathcal{S}(\Omega, r) = \{A \in \mathcal{P}(E) : d(\Omega, A) = r\} \quad \text{et} \quad \mathcal{B}(\Omega, r) = \{A \in \mathcal{P}(E) : d(\Omega, A) \leq r\}.$$

$\alpha]$ Démontrer que

$$\text{card}(\mathcal{S}(\Omega, r)) = \binom{n}{r}.$$

$\beta]$ En déduire la valeur (sous forme d'une somme) du cardinal de $\mathcal{B}(\Omega, r)$.

3. Codage de Hamming

Soient $p, r \in \mathbb{N}^*$. On considère un « codage de Hamming d'isolement r », c'est-à-dire la donnée d'un entier $n \in \mathbb{N}^*$ tel que $n \geq p$ et d'une application $\Phi : \mathcal{P}(\llbracket 1; p \rrbracket) \longrightarrow \mathcal{P}(\llbracket 1; n \rrbracket)$ telle que

$$\forall X, Y \in \mathcal{P}(\llbracket 1; p \rrbracket), \quad (X \neq Y) \implies (d(\Phi(X), \Phi(Y)) > 2r),$$

où d désigne la distance de Hamming sur $\mathcal{P}(\llbracket 1; n \rrbracket)$.

- a) Soient $X, Y \in \mathcal{P}(\llbracket 1; p \rrbracket)$ telles que $X \neq Y$. Démontrer que les boules $\mathcal{B}(\Phi(X), r)$ et $\mathcal{B}(\Phi(Y), r)$ sont disjointes.

Quelle propriété de Φ déduit-on simplement de ce résultat ?

- b) Démontrer l'inégalité dite « de la borne de Hamming » :

$$2^p \leq \frac{2^n}{\sum_{k=0}^r \binom{n}{k}}.$$

- c) Pour un entier $r \in \mathbb{N}^*$ fixé, on dit que le codage de Hamming est parfait lorsqu'il y a égalité dans l'inégalité de la borne de Hamming.

On suppose que $r = 1$. Démontrer que le codage de Hamming est parfait si, et seulement si, il existe $k \in \mathbb{N} \setminus \{0; 1\}$ tel que $(p, n) = (2^k - 1 - k, 2^k - 1)$.

Explications :

On décide de représenter un message de p bits par la partie X de $\llbracket 1; p \rrbracket$ contenant les positions des chiffres 1 dans le message. Ainsi, lorsque $p = 7$, le message 1001101 est représenté par la partie $X = \{1, 4, 5, 7\}$.

Pour remédier aux problèmes de parasitage lors de sa transmission du message, on transforme (= on code) le message X en $\Phi(X)$ puis on transmet $\Phi(X)$. Si une petite erreur survient lors de la transmission, le récepteur reçoit un message proche de $\Phi(X)$, ce qui lui permet d'identifier $\Phi(X)$ puisque chaque $\Phi(X)$ est « isolé » dans la boule $\mathcal{B}(\Phi(X), r)$. Ainsi, le récepteur peut repérer et éventuellement corriger l'erreur (ou demander une nouvelle émission du message). Il lui reste alors à décoder $\Phi(X)$ en X pour récupérer le message de départ.

CORRECTION DU DS 3

(durée : 3 h 30)

EXERCICE 1

Une séquence de Skolem d'ordre n est un $2n$ -uplet constitué des entiers de 1 à n répétés chacun deux fois, tel que, pour tout $k \in \llbracket 1; n \rrbracket$, les deux apparitions de l'entier k soient distantes de k . Par exemple, $(4, 5, 1, 1, 4, 3, 5, 2, 3, 2)$ est une séquence de Skolem d'ordre 5 puisque les deux 1 sont distants d'une unité, les deux 2 sont distants de deux unités, les deux 3 sont distants de trois unités, les deux 4 sont distants de quatre unités et les deux 5 sont distants de cinq unités. On se donne une séquence de Skolem d'ordre n (où $n \in \mathbb{N}^*$), c'est-à-dire une famille $(x_i)_{1 \leq i \leq 2n}$ d'entiers dans $\llbracket 1; n \rrbracket$ telle que, pour tout nombre $k \in \llbracket 1; n \rrbracket$, il existe exactement deux indices distincts a_k et b_k dans $\llbracket 1; 2n \rrbracket$ tels que $b_k - a_k = k$ et $x_{a_k} = x_{b_k} = k$. On notera, qu'avec ces notations, on a $a_k < b_k$ autrement dit que a_k est le premier rang où l'on rencontre k et b_k est le second.

- Pour la séquence de Skolem $(4, 5, 1, 1, 4, 3, 5, 2, 3, 2)$, donner $a_1, b_1, a_2, b_2, a_3, b_3, a_4, b_4, a_5, b_5$.

On a

$$a_1 = 3, b_1 = 4, a_2 = 8, b_2 = 10, a_3 = 6, b_3 = 9, a_4 = 1, b_4 = 5, a_5 = 2, b_5 = 7.$$

- Justifier que $\sum_{k=1}^n a_k + \sum_{k=1}^n b_k = n(2n+1)$.

En additionnant tous les a_k et tous les b_k , on obtient la somme de tous les indices des termes de la séquence de Skolem, c'est-à-dire la somme de tous les entiers entre 1 et $2n$. Donc

$$\sum_{k=1}^n a_k + \sum_{k=1}^n b_k = 1 + 2 + 3 + \cdots + 2n = \frac{2n(2n+1)}{2} = n(2n+1).$$

Comme $\forall k \in \llbracket 1; n \rrbracket, b_k = a_k + k$, on a

$$\sum_{k=1}^n b_k = \sum_{k=1}^n (a_k + k) = \sum_{k=1}^n a_k + \sum_{k=1}^n k = \sum_{k=1}^n a_k + \frac{n(n+1)}{2}.$$

En combinant ces résultats, on obtient

$$\sum_{k=1}^n a_k + \sum_{k=1}^n a_k + \frac{n(n+1)}{2} = n(2n+1),$$

c'est-à-dire

$$2 \sum_{k=1}^n a_k = n(2n+1) - \frac{n(n+1)}{2}.$$

Comme

$$n(2n+1) - \frac{n(n+1)}{2} = 2n^2 + n - \frac{n^2 + n}{2} = 2n^2 - \frac{n^2 - n}{2} = 2n^2 - \frac{n(n-1)}{2},$$

on obtient finalement

$$\sum_{k=1}^n a_k = n^2 - \frac{n(n-1)}{4}.$$

3. En déduire que n ou $n - 1$ est un multiple de 4.

Comme $\sum_{k=1}^n a_k$ est une somme de nombres entiers et comme n^2 est également un entier, on déduit de la question précédente que

$$\frac{n(n-1)}{4} \in \mathbb{Z}.$$

Cela signifie que, parmi les deux nombres consécutifs $n - 1$ et n , celui des deux qui est pair est en fait divisible par 4. Donc

n ou $n - 1$ est un multiple de 4.

EXERCICE 2

Soit $n \in \mathbb{N}^*$. On pose $\omega = e^{2i\pi/n}$. Si u est un n -uplet de \mathbb{C}^n , on note $u = (u_0, u_1, \dots, u_{n-1})$ ou encore $u = (u_k)_{k \in \llbracket 0; n-1 \rrbracket}$. De plus, on pose $u_{-1} = u_{n-1}$, $u_{-2} = u_{n-2}$, ..., $u_{-(n-1)} = u_1$. Pour tous n -uplets u, v de \mathbb{C}^n , on appelle produit de convolution discret de u et v le n -uplet $u \otimes v = (a_0, a_1, \dots, a_{n-1})$ de \mathbb{C}^n défini par $\forall j \in \llbracket 0; n-1 \rrbracket$, $a_j = \sum_{k=0}^{n-1} u_k v_{j-k}$. On considère la transformée de Fourier discrète sur \mathbb{C}^n , c'est-à-dire l'application $F : \mathbb{C}^n \rightarrow \mathbb{C}^n$ telle que $F : (u_0, u_1, \dots, u_{n-1}) \mapsto (b_0, b_1, \dots, b_{n-1})$ avec $\forall k \in \llbracket 0; n-1 \rrbracket$, $b_k = \sum_{j=0}^{n-1} \overline{u_j} \omega^{kj}$. On rappelle que $(\mathbb{C}^n, +, \times)$ est un anneau commutatif (où $+$ et \times sont respectivement l'addition et la multiplication terme à terme). On admet que $(\mathbb{C}^n, +, \otimes)$ est également un anneau commutatif.

1. a) Soit $m \in \mathbb{Z}$. Calculer $\sum_{j=0}^{n-1} \omega^{mj}$.

La somme $\sum_{j=0}^{n-1} \omega^{mj}$ est géométrique de raison ω^m . On distingue alors deux cas.

▷ Premier cas : Si $\omega^m = 1$ c'est-à-dire si n divise m , on a

$$\sum_{j=0}^{n-1} \omega^{mj} = \sum_{j=0}^{n-1} 1 = n.$$

▷ Second cas : Si $\omega^m \neq 1$, on a

$$\sum_{j=0}^{n-1} \omega^{mj} = \frac{\omega^{mn} - 1}{\omega^m - 1} = \frac{(\omega^n)^m - 1}{\omega^m - 1} = \frac{1^m - 1}{\omega^m - 1} = 0.$$

En conclusion, on a

$$\sum_{j=0}^{n-1} \omega^{mj} = \begin{cases} n & \text{si } m \text{ est un multiple de } n, \\ 0 & \text{sinon.} \end{cases}$$

- b) Soient $k, p \in \llbracket 0; n-1 \rrbracket$ et $u \in \mathbb{C}^n$. Démontrer que $\sum_{j=-p}^{n-1-p} \overline{u_j} \omega^{kj} = \sum_{j=0}^{n-1} \overline{u_j} \omega^{kj}$.

On a

$$\begin{aligned} \sum_{j=-p}^{n-1-p} \overline{u_j} \omega^{kj} &= \sum_{j=-p}^{-1} \overline{u_j} \omega^{kj} + \sum_{j=0}^{n-1-p} \overline{u_j} \omega^{kj} \\ &= \sum_{i=n-p}^{n-1} \overline{u_{i-n}} \omega^{k(i-n)} + \sum_{j=0}^{n-1-p} \overline{u_j} \omega^{kj} \quad \text{en posant } i = n + j \\ &= \sum_{i=n-p}^{n-1} \overline{u_i} \omega^{ki} + \sum_{j=0}^{n-1-p} \overline{u_j} \omega^{kj} \quad \text{car } u_{i-n} = u_i \text{ et} \\ &\quad \omega^{-kn} = (\omega^n)^{-k} = 1 \\ &= \sum_{j=0}^{n-1} \overline{u_j} \omega^{kj}, \end{aligned}$$

donc

$$\sum_{j=-p}^{n-1-p} \overline{u_j} \omega^{kj} = \sum_{j=0}^{n-1} \overline{u_j} \omega^{kj}.$$

c) Quel est l'élément neutre pour \otimes ?

Pour tout $(u_0, u_1, \dots, u_{n-1}) \in \mathbb{C}^n$, on a

$$\begin{aligned}(u_0, u_1, \dots, u_{n-1}) \otimes (1, 0, \dots, 0) &= (u_0 \times 0 + u_1 \times 0 + \dots + u_j \times 1 + \dots + u_{n-1} \times 0)_{j \in \llbracket 0; n-1 \rrbracket} \\ &= (u_j)_{j \in \llbracket 0; n-1 \rrbracket} \\ &= (u_0, u_1, \dots, u_{n-1})\end{aligned}$$

donc, comme \otimes est commutative, on en conclut que

$$\boxed{\text{l'élément neutre pour } \otimes \text{ est } (1, 0, \dots, 0).}$$

2. Calculer $F \circ F$. En déduire que F est une bijection dont on précisera la réciproque.

Soit $u = (u_0, u_1, \dots, u_{n-1}) \in \mathbb{C}^n$. On a

$$\begin{aligned}(F \circ F)(u) &= F \left(\left(\sum_{j=0}^{n-1} \overline{u_j} \omega^{kj} \right)_{k \in \llbracket 0; n-1 \rrbracket} \right) \\ &= \left(\sum_{k=0}^{n-1} \sum_{j=0}^{n-1} \overline{u_j} \omega^{kj} \omega^{\ell k} \right)_{\ell \in \llbracket 0; n-1 \rrbracket} \\ &= \left(\sum_{k=0}^{n-1} \sum_{j=0}^{n-1} u_j \omega^{-kj} \omega^{\ell k} \right)_{\ell \in \llbracket 0; n-1 \rrbracket} \\ &= \left(\sum_{j=0}^{n-1} u_j \sum_{k=0}^{n-1} \omega^{(\ell-j)k} \right)_{\ell \in \llbracket 0; n-1 \rrbracket} \quad \text{par Fubini.}\end{aligned}$$

Or, d'après la question 1.a), on a

$$\sum_{k=0}^{n-1} \omega^{(\ell-j)k} = \begin{cases} n & \text{si } \ell = j, \\ 0 & \text{sinon,} \end{cases}$$

donc

$$(F \circ F)(u) = (nu_\ell)_{\ell \in \llbracket 0; n-1 \rrbracket} = nu.$$

On a ainsi démontré que

$$\boxed{F \circ F = n \text{ Id}_{\mathbb{C}^n}.}$$

On en déduit immédiatement que

$$\boxed{F \text{ est une bijection et } F^{-1} = \frac{1}{n} F.}$$

3. a) Démontrer que, pour tous $u, v \in \mathbb{C}^n$, on a $F(u+v) = F(u) + F(v)$.

Pour tous $u, v \in \mathbb{C}^n$, on a

$$\begin{aligned}F(u+v) &= \left(\sum_{j=0}^{n-1} \overline{u_j + v_j} \omega^{kj} \right)_{k \in \llbracket 0; n-1 \rrbracket} \\ &= \left(\sum_{j=0}^{n-1} (\overline{u_j} + \overline{v_j}) \omega^{kj} \right)_{k \in \llbracket 0; n-1 \rrbracket} \\ &= \left(\sum_{j=0}^{n-1} \overline{u_j} \omega^{kj} + \sum_{j=0}^{n-1} \overline{v_j} \omega^{kj} \right)_{k \in \llbracket 0; n-1 \rrbracket} \\ &= \left(\sum_{j=0}^{n-1} \overline{u_j} \omega^{kj} \right)_{k \in \llbracket 0; n-1 \rrbracket} + \left(\sum_{j=0}^{n-1} \overline{v_j} \omega^{kj} \right)_{k \in \llbracket 0; n-1 \rrbracket} \\ &= F(u) + F(v),\end{aligned}$$

donc

$$\boxed{\forall u, v \in \mathbb{C}^n, \quad F(u+v) = F(u) + F(v).}$$

b) Démontrer que, pour tous $u, v \in \mathbb{C}^n$, on a $F(u \otimes v) = F(u) \times F(v)$.

Pour tous $u, v \in \mathbb{C}^n$, on a

$$\begin{aligned}
F(u \otimes v) &= \left(\sum_{j=0}^{n-1} \overline{(u \otimes v)_j} \omega^{kj} \right)_{k \in \llbracket 0; n-1 \rrbracket} \\
&= \left(\sum_{j=0}^{n-1} \sum_{p=0}^{n-1} u_p v_{j-p} \omega^{kj} \right)_{k \in \llbracket 0; n-1 \rrbracket} \\
&= \left(\sum_{j=0}^{n-1} \sum_{p=0}^{n-1} \overline{u_p} \overline{v_{j-p}} \omega^{kj} \right)_{k \in \llbracket 0; n-1 \rrbracket} \\
&= \left(\sum_{p=0}^{n-1} \overline{u_p} \sum_{j=0}^{n-1} \overline{v_{j-p}} \omega^{kj} \right)_{k \in \llbracket 0; n-1 \rrbracket} \quad \text{par Fubini} \\
&= \left(\sum_{p=0}^{n-1} \overline{u_p} \sum_{\ell=-p}^{n-1-p} \overline{v_\ell} \omega^{k(\ell+p)} \right)_{k \in \llbracket 0; n-1 \rrbracket} \quad \text{en posant } \ell = j - p \\
&= \left(\sum_{p=0}^{n-1} \overline{u_p} \omega^{kp} \sum_{\ell=-p}^{n-1-p} \overline{v_\ell} \omega^{k\ell} \right)_{k \in \llbracket 0; n-1 \rrbracket} \\
&= \left(\sum_{p=0}^{n-1} \overline{u_p} \omega^{kp} \sum_{\ell=0}^{n-1} \overline{v_\ell} \omega^{k\ell} \right)_{k \in \llbracket 0; n-1 \rrbracket} \quad \text{d'après 1. b)} \\
&= \left(\sum_{p=0}^{n-1} \overline{u_p} \omega^{kp} \times \sum_{\ell=0}^{n-1} \overline{v_\ell} \omega^{k\ell} \right)_{k \in \llbracket 0; n-1 \rrbracket} \\
&= \left(\sum_{p=0}^{n-1} \overline{u_p} \omega^{kp} \right)_{k \in \llbracket 0; n-1 \rrbracket} \times \left(\sum_{\ell=0}^{n-1} \overline{v_\ell} \omega^{k\ell} \right)_{k \in \llbracket 0; n-1 \rrbracket} \\
&= F(u) \times F(v),
\end{aligned}$$

donc

$$\boxed{\forall u, v \in \mathbb{C}^n, \quad F(u \otimes v) = F(u) \times F(v).}$$

c) Démontrer que F est un isomorphisme d'anneaux entre $(\mathbb{C}^n, +, \otimes)$ et $(\mathbb{C}^n, +, \times)$.

La question 2 nous dit que F est une bijection. Il reste donc à démontrer que F est un morphisme d'anneaux, c'est-à-dire

$$F((1, 0, \dots, 0)) = (1, 1, \dots, 1),$$

$$\forall u, v \in \mathbb{C}^n, \quad F(u + v) = F(u) + F(v)$$

et

$$\forall u, v \in \mathbb{C}^n, \quad F(u \otimes v) = F(u) \times F(v).$$

Les deux dernières propriétés ont été démontrées en 3. a) et 3. b). Il ne reste plus qu'à démontrer la première. Allons-y ! On a

$$\begin{aligned}
F((1, 0, \dots, 0)) &= (\overline{1} \omega^{k \cdot 0} + \overline{0} \omega^{k \cdot 1} + \dots + \overline{0} \omega^{k \cdot (n-1)})_{k \in \llbracket 0; n-1 \rrbracket} \\
&= (1)_{k \in \llbracket 0; n-1 \rrbracket} \\
&= (1, 1, \dots, 1).
\end{aligned}$$

En conclusion,

$$\boxed{F \text{ est un isomorphisme d'anneaux entre } (\mathbb{C}^n, +, \otimes) \text{ et } (\mathbb{C}^n, +, \times).}$$

4. Soient $u, v \in \mathbb{C}^n$. Déterminer une condition nécessaire et suffisante pour que l'équation $u \otimes x = v$ d'inconnue $x \in \mathbb{C}^n$ admette au moins une solution.

Pour tout $x \in \mathbb{C}^n$, on a

$$\begin{aligned} u \otimes x &= v \\ \iff F(u \otimes x) &= F(v) \quad \text{car } F \text{ est injective} \\ \iff F(u) \times F(x) &= F(v) \quad \text{d'après 3. b)} \\ \iff \forall k \in \llbracket 0; n-1 \rrbracket, \quad F(u)_k \times F(x)_k &= F(v)_k \quad \begin{array}{l} \text{où } F(\cdot)_k \text{ désigne le } k\text{-ème} \\ \text{élément du } n\text{-uplet } F(\cdot) \end{array} \\ \iff \forall k \in \llbracket 0; n-1 \rrbracket, \quad \left\{ \begin{array}{ll} F(x)_k = \frac{F(v)_k}{F(u)_k} & \text{si } F(u)_k \neq 0 \\ F(x)_k \text{ n'existe pas} & \text{si } F(u)_k = 0 \text{ et } F(v)_k \neq 0 \\ F(x)_k \text{ est quelconque} & \text{si } F(u)_k = 0 \text{ et } F(v)_k = 0 \end{array} \right. \end{aligned}$$

Donc

l'équation $u \otimes x = v$ d'inconnue $x \in \mathbb{C}^n$ admet au moins une solution si et seulement si $\forall k \in \llbracket 0; n-1 \rrbracket, (F(u)_k = 0) \Rightarrow (F(v)_k = 0)$.

EXERCICE 3

Au Loto Foot 15, le parieur remplit une grille dans laquelle il indique ses prévisions pour quinze matchs de football à venir. Pour chacun des matchs, il peut cocher au choix trois cases : 1, 2 ou N.

1. De combien de façons un parieur peut-il remplir la grille ?

Pour remplir une grille, le parieur choisit successivement :

- ▷ une case parmi 3 pour le premier match : 3 choix ;
- ▷ une case parmi 3 pour le deuxième match : 3 choix ;
- ⋮
- ▷ une case parmi 3 pour le quinzième match : 3 choix.

Par conséquent,

il y a 3^{15} façons de remplir une grille.

2. Pour gagner, il faut cocher au moins douze bonnes réponses. Quel est le nombre de grilles gagnantes ?

Pour gagner, le parieur doit donc avoir coché une grille avec exactement 12 bonnes réponses ou exactement 13 bonnes réponses ou exactement 14 bonnes réponses ou exactement 15 bonnes réponses.

- ▶ Pour dénombrer le nombre de grilles avec 12 bonnes réponses, on choisit successivement :
 - ▷ les 12 matchs parmi 15 pour lesquels le pronostic sera exact : $\binom{15}{12}$ choix ;
 - ▷ Pour ces 12 matchs, le parieur aura choisi la bonne réponse : 1 possibilité à chaque fois ;
 - ▷ Pour les 3 autres matchs, le parieur aura choisi une des deux mauvaises réponses, ce qui offre 2 possibilités pour chacun de ces matchs, c'est-à-dire 2^3 choix.

Il y a donc $\binom{15}{12}2^3$ grilles avec exactement 12 réponses exactes.

- ▶ En procédant de même, on trouve $\binom{15}{13}2^2$ grilles avec 13 bonnes réponses, $\binom{15}{14}2^1$ grilles avec 14 bonnes réponses et $\binom{15}{15}2^0$ grilles avec 15 bonnes réponses correctes.

En définitive,

il y a $\binom{15}{12}2^3 + \binom{15}{13}2^2 + \binom{15}{14}2^1 + \binom{15}{15}2^0 = 4091$ grilles gagnantes.

EXERCICE 4

L'objet de cet exercice est de présenter les bases théoriques du codage de Hamming.

1. Soit E un ensemble fini de cardinal n (où $n \in \mathbb{N}^*$). Pour A et B deux parties de E , on définit la différence symétrique de A et B , notée $A\Delta B$, par $A\Delta B = (A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A)$. En exercice, nous avons démontré que Δ est une opération associative et commutative ; que, pour toutes parties A et B de E , on a $A\Delta A = \emptyset$ et même, plus précisément, $(A\Delta B = \emptyset) \iff (A = B)$ et enfin que \cap est distributive sur Δ . Ces propriétés sont supposées acquises.

- a) Justifier $(\mathcal{P}(E), \Delta, \cap)$ est un anneau commutatif. On précisera les éléments neutres et, pour tout $A \in \mathcal{P}(E)$, on donnera le symétrique de A pour la loi Δ .

La loi Δ est interne sur $\mathcal{P}(E)$, associative et commutative. Son élément neutre est \emptyset puisque, pour tout $A \in \mathcal{P}(E)$, on a $A\Delta\emptyset = (A \cup \emptyset) \setminus (A \cap \emptyset) = A \setminus \emptyset = A$. Enfin, comme $A\Delta A = \emptyset$ pour tout $A \in \mathcal{P}(E)$, on sait que tout élément de $\mathcal{P}(E)$ est symétrisable pour Δ et que le symétrique d'un élément est lui-même. On en déduit que (A, Δ) est un groupe abélien.

La loi \cap est interne sur $\mathcal{P}(E)$, associative et commutative. Son élément neutre est E puisque, pour tout $A \in \mathcal{P}(E)$, on a $A \cap E = A$. Ainsi, (A, \cap) est un monoïde commutatif.

Enfin, on sait que \cap est distributive sur Δ .

En conclusion,

$(\mathcal{P}(E), \Delta, \cap)$ est un anneau commutatif dont les éléments neutres sont \emptyset pour Δ et E pour \cap et dans lequel tout élément est égal à son symétrique (pour la loi Δ).

- b) Déterminer $U(\mathcal{P}(E))$, c'est-à-dire le groupe des éléments inversibles de $\mathcal{P}(E)$. L'anneau $(\mathcal{P}(E), \Delta, \cap)$ est-il un corps ?

On a

$$(A \in U(\mathcal{P}(E))) \iff (\exists B \in \mathcal{P}(E), A \cap B = E) \iff (A = E),$$

donc

$$U(\mathcal{P}(E)) = \{E\}.$$

On a

$$\begin{aligned} ((\mathcal{P}(E), \Delta, \cap) \text{ est un corps}) &\iff (U(\mathcal{P}(E)) = \mathcal{P}(E) \setminus \{\emptyset\} \text{ et } \mathcal{P}(E) \neq \{\emptyset\}) \\ &\iff (\mathcal{P}(E) = \{\emptyset, E\} \text{ et } \mathcal{P}(E) \neq \{\emptyset\}) \\ &\iff (E \text{ est un singleton}), \end{aligned}$$

donc

$$\text{l'anneau } (\mathcal{P}(E), \Delta, \cap) \text{ est un corps si, et seulement si, } n = 1.$$

- c) a] Soit $A \in \mathcal{P}(E)$. Démontrer que $\mathcal{P}(A)$ est un idéal de $\mathcal{P}(E)$.

On a $\emptyset \in \mathcal{P}(A)$. Si $X, Y \in \mathcal{P}(A)$ alors $X\Delta Y \in \mathcal{P}(A)$ et le symétrique de X (pour Δ) est bien dans $\mathcal{P}(A)$ puisque c'est X lui-même. Ainsi, $(\mathcal{P}(A), \Delta)$ est un sous-groupe de $(\mathcal{P}(E), \Delta)$.

Soit $X \in \mathcal{P}(A)$ et $Y \in \mathcal{P}(E)$. Comme $X \cap Y \subset X$, on a $X \cap Y \in \mathcal{P}(A)$. Cela prouve l'hyperstabilité de $\mathcal{P}(A)$ pour la loi \cap .

En conclusion,

$$\mathcal{P}(A) \text{ est un idéal de } \mathcal{P}(E).$$

- b] Soit \mathcal{I} un idéal de l'anneau $\mathcal{P}(E)$. Démontrer que $\forall X \in \mathcal{I}, \forall Y \subset X, Y \in \mathcal{I}$ et $\forall X, Y \in \mathcal{I}, X \cup Y \in \mathcal{I}$. En déduire l'existence de $A \in \mathcal{P}(E)$ tel que $\mathcal{I} = \mathcal{P}(A)$.

Soient $X \in \mathcal{I}$ et $Y \subset X$. On a $Y = X \cap Y$. Or $X \cap Y \in \mathcal{I}$ par hyperstabilité de \mathcal{I} pour la loi \cap , donc $Y \in \mathcal{I}$. Par conséquent, on a

$$\forall X \in \mathcal{I}, \forall Y \subset X, Y \in \mathcal{I}$$

Soient $X, Y \in \mathcal{I}$. On sait que $X\Delta Y$ appartient à \mathcal{I} puisque (\mathcal{I}, Δ) est un groupe. Or $X \setminus Y$ est inclus dans $X\Delta Y$ donc, d'après le résultat ci-dessus, on en déduit que $X \setminus Y$ appartient à \mathcal{I} . Il s'ensuit que $(X \setminus Y)\Delta Y$ appartient à \mathcal{I} (à nouveau parce que (\mathcal{I}, Δ) est un groupe). Or $(X \setminus Y)\Delta Y = X \cup Y$, donc $X \cup Y$ appartient à \mathcal{I} . Ainsi,

$$\boxed{\forall X, Y \in \mathcal{I}, \quad X \cup Y \in \mathcal{I}.}$$

Posons

$$A = \bigcup_{X \in \mathcal{I}} X$$

et démontrons que $\mathcal{I} = \mathcal{P}(A)$ par double inclusion.

\subset Soit $X \in \mathcal{I}$. Alors X est l'une des parties de l'union $\bigcup_{X \in \mathcal{I}} X$ et donc $X \subset A$, c'est-à-dire $X \in \mathcal{P}(A)$. Donc $\mathcal{I} \subset \mathcal{P}(A)$.

\supset Comme E est fini, $\mathcal{P}(E)$ l'est aussi (on sait même que $\text{card } \mathcal{P}(E) = 2^n$). Il s'ensuit que l'union $\bigcup_{X \in \mathcal{I}} X$ est une union finie d'éléments de \mathcal{I} . Or nous venons de voir que \mathcal{I} est stable par union finie (on l'a démontré pour deux éléments de \mathcal{I} et il est facile de généraliser ce résultat à un nombre fini d'éléments de \mathcal{I} à l'aide d'une récurrence immédiate). Dès lors, on a $A \in \mathcal{I}$. Mézalors, d'après la première propriété démontrée dans cette question, on en déduit que toute partie de A est dans \mathcal{I} , autrement dit que $\mathcal{P}(A) \subset \mathcal{I}$.

En conclusion,

$$\boxed{\text{il existe } A \in \mathcal{P}(E) \text{ tel que } \mathcal{I} = \mathcal{P}(A).}$$

2. Soit E un ensemble fini de cardinal n (où $n \in \mathbb{N}^*$). Pour A et B deux parties de E , on définit la distance de Hamming $d(A, B)$ entre A et B par $d(A, B) = \text{card}(A\Delta B)$.

a) Démontrer que la distance de Hamming $d : \mathcal{P}(E)^2 \rightarrow \mathbb{R}$ est une métrique sur $\mathcal{P}(E)$, autrement dit que : (i) $\forall A, B \in \mathcal{P}(E)$, $d(A, B) \geq 0$; (ii) $\forall A, B \in \mathcal{P}(E)$, $d(A, B) = d(B, A)$; (iii) $\forall A, B \in \mathcal{P}(E)$, $d(A, B) = 0 \Leftrightarrow A = B$; (iv) $\forall A, B, C \in \mathcal{P}(E)$, $d(A, C) \leq d(A, B) + d(B, C)$. On dit alors que le couple $(\mathcal{P}(E), d)$ est un espace métrique.

Démontrons successivement les propriétés (i) à (iv).

- (i) Pour $A, B \in \mathcal{P}(E)$, on a $d(A, B) = \text{card}(A\Delta B) \in \mathbb{N}$, donc $d(A, B) \geq 0$. Cela démontre l'axiome de positivité.
- (ii) Pour $A, B \in \mathcal{P}(E)$, on a $d(A, B) = \text{card}(A\Delta B) = \text{card}(B\Delta A) = d(B, A)$ où l'on a utilisé la commutativité de la loi Δ . Cela démontre l'axiome de symétrie.
- (iii) Pour $A, B \in \mathcal{P}(E)$, on a $(d(A, B) = 0) \Leftrightarrow (\text{card}(A\Delta B) = 0) \Leftrightarrow (A\Delta B = \emptyset) \Leftrightarrow (A = B)$. Cela démontre l'axiome de séparation.
- (iv) Pour $A, B, C \in \mathcal{P}(E)$, on a

$$\begin{aligned}
 d(A, C) &= \text{card}(A\Delta C) \\
 &= \text{card}(A\Delta(B\Delta B)\Delta C) && \text{car } B\Delta B = \emptyset \text{ et} \\
 &= \text{card}((A\Delta B)\Delta(B\Delta C)) && \emptyset \text{ est neutre pour } \Delta \\
 &\leq \text{card}((A\Delta B) \cup (B\Delta C)) && \text{par associativité de } \Delta \\
 &\leq \text{card}(A\Delta B) + \text{card}(B\Delta C) && \text{car } (A\Delta B)\Delta(B\Delta C) \text{ est} \\
 & && \text{inclus dans } (A\Delta B) \cup (B\Delta C) \\
 & && \text{car le cardinal d'une union} \\
 & && \text{est inférieur ou égal à la} \\
 & && \text{somme des cardinaux} \\
 &= d(A, B) + d(B, C).
 \end{aligned}$$

Cela démontre l'inégalité triangulaire.

En conclusion,

$$\boxed{\text{la distance de Hamming } d \text{ est une métrique sur } \mathcal{P}(E).}$$

- b) Soient $\Omega \in \mathcal{P}(E)$ et $r \in \mathbb{N}$. Dans l'espace métrique $(\mathcal{P}(E), d)$, on définit la sphère $\mathcal{S}(\Omega, r)$ de centre Ω et de rayon r ainsi que la boule $\mathcal{B}(\Omega, r)$ de centre Ω et de rayon r de la façon suivante : $\mathcal{S}(\Omega, r) = \{A \in \mathcal{P}(E) : d(\Omega, A) = r\}$ et $\mathcal{B}(\Omega, r) = \{A \in \mathcal{P}(E) : d(\Omega, A) \leq r\}$.

a] Démontrer que $\text{card}(\mathcal{S}(\Omega, r)) = \binom{n}{r}$.

Remarquons tout d'abord que si $\Omega = \emptyset$, on a

$$\begin{aligned}\mathcal{S}(\emptyset, r) &= \{A \in \mathcal{P}(E) : d(\emptyset, A) = r\} \\ &= \{A \in \mathcal{P}(E) : \text{card}(\emptyset \Delta A) = r\} \\ &= \{A \in \mathcal{P}(E) : \text{card}(A) = r\}.\end{aligned}$$

Comme l'ensemble des parties de E de cardinal r est l'ensemble des r -combinaisons de E , le cours nous dit que

$$\text{card}(\mathcal{S}(\emptyset, r)) = \binom{n}{r}.$$

Reste alors à généraliser ce résultat aux autres sphères de $\mathcal{P}(E)$. Pour cela, nous allons translater ! (pour la loi additive de l'anneau $\mathcal{P}(E)$, c'est-à-dire la loi Δ). Considérons l'application

$$T_\Omega \begin{cases} \mathcal{P}(E) & \longrightarrow \mathcal{P}(E) \\ X & \longmapsto X\Delta\Omega \end{cases}$$

C'est une involution de $\mathcal{P}(E)$, c'est-à-dire une bijection entre $\mathcal{P}(E)$ et lui-même qui est égale à sa propre réciproque. En effet, pour tout $X \in \mathcal{P}(E)$, on a

$$(T_\Omega \circ T_\Omega)(X) = (X\Delta\Omega)\Delta\Omega = X\Delta(\Omega\Delta\Omega) = X\Delta\emptyset = X.$$

De plus, il est clair que

$$T_\Omega(\mathcal{S}(\emptyset, r)) = \mathcal{S}(\Omega, r)$$

donc

$$T_\Omega \Big|_{\mathcal{S}(\emptyset, r)}^{\mathcal{S}(\Omega, r)} \text{ est une bijection.}$$

Il s'ensuit que

$$\text{card}(\mathcal{S}(\Omega, r)) = \text{card}(\mathcal{S}(\emptyset, r))$$

et donc

$$\boxed{\text{card}(\mathcal{S}(\Omega, r)) = \binom{n}{r}}.$$

- β] En déduire la valeur (sous forme d'une somme) du cardinal de $\mathcal{B}(\Omega, r)$.

La boule $\mathcal{B}(\Omega, r)$ est la réunion disjointe des sphères $\mathcal{S}(\Omega, k)$ pour k parcourant l'intervalle d'entiers $\llbracket 0; r \rrbracket$, donc

$$\boxed{\text{card}(\mathcal{B}(\Omega, r)) = \sum_{k=0}^r \binom{n}{k}}.$$

3. Soient $p, r \in \mathbb{N}^*$. On considère un « codage de Hamming d'isolement r », c'est-à-dire la donnée d'un entier $n \in \mathbb{N}^*$ tel que $n \geq p$ et d'une application $\Phi : \mathcal{P}(\llbracket 1; p \rrbracket) \longrightarrow \mathcal{P}(\llbracket 1; n \rrbracket)$ telle que $\forall X, Y \in \mathcal{P}(\llbracket 1; p \rrbracket)$, $X \neq Y \Rightarrow d(\Phi(X), \Phi(Y)) > 2r$, où d est la distance de Hamming sur $\mathcal{P}(\llbracket 1; n \rrbracket)$.

- a) Soient $X, Y \in \mathcal{P}(\llbracket 1; p \rrbracket)$ telles que $X \neq Y$. Démontrer que les boules $\mathcal{B}(\Phi(X), r)$ et $\mathcal{B}(\Phi(Y), r)$ sont disjointes. Quelle propriété de Φ déduit-on simplement de ce résultat ?

Par l'absurde, supposons qu'il existe $Z \in \mathcal{B}(\Phi(X), r) \cap \mathcal{B}(\Phi(Y), r)$. On a alors

$$d(\Phi(X), Z) \leq r \quad \text{et} \quad d(\Phi(Y), Z) \leq r.$$

Mézalors, d'après l'inégalité triangulaire, on a

$$d(\Phi(X), \Phi(Y)) \leq d(\Phi(X), Z) + d(Z, \Phi(Y)) \leq 2r,$$

ce qui contredit l'hypothèse faite sur Φ . C'est absurde ! Donc

$$\boxed{\text{les boules } \mathcal{B}(\Phi(X), r) \text{ et } \mathcal{B}(\Phi(Y), r) \text{ sont disjointes.}}$$

Cette propriété implique en particulier que

$$\forall X, Y \in \mathcal{P}(\llbracket 1; p \rrbracket), \quad (X \neq Y) \implies (\Phi(X) \neq \Phi(Y))$$

donc

Φ est injective.

b) Démontrer l'inégalité dite « de la borne de Hamming » : $2^p \leq 2^n / \sum_{k=0}^r \binom{n}{k}$.

La réunion des boules de $\mathcal{P}(\llbracket 1; n \rrbracket)$ de rayon r dont le centre est un élément de $\Phi(\mathcal{P}(\llbracket 1; p \rrbracket))$ est une partie de $\mathcal{P}(\llbracket 1; n \rrbracket)$, donc

$$\text{card} \left(\bigcup_{X \in \mathcal{P}(\llbracket 1; p \rrbracket)} \mathcal{B}(\Phi(X), r) \right) \leq \text{card}(\mathcal{P}(\llbracket 1; n \rrbracket)).$$

Comme la question 3.a) nous dit que les boules de $\mathcal{P}(\llbracket 1; n \rrbracket)$ de rayon r dont le centre est un élément de $\Phi(\mathcal{P}(\llbracket 1; p \rrbracket))$ sont disjointes deux à deux et comme, par ailleurs, $\mathcal{P}(\llbracket 1; n \rrbracket)$ est de cardinal 2^n , on en déduit que

$$\sum_{X \in \mathcal{P}(\llbracket 1; p \rrbracket)} \text{card}(\mathcal{B}(\Phi(X), r)) \leq 2^n.$$

Or la question 2.b) β] nous dit que toutes les boules $\mathcal{B}(\Phi(X), r)$ où X parcourt $\mathcal{P}(\llbracket 1; p \rrbracket)$ ont toutes le même cardinal, à savoir $\sum_{k=0}^r \binom{n}{k}$. De plus, on sait que $\mathcal{P}(\llbracket 1; p \rrbracket)$ est de cardinal 2^p .

L'inégalité ci-dessus devient donc

$$2^p \sum_{k=0}^r \binom{n}{k} \leq 2^n,$$

c'est-à-dire

$$2^p \leq \frac{2^n}{\sum_{k=0}^r \binom{n}{k}}.$$

- c) Pour un entier $r \in \mathbb{N}^*$ fixé, on dit que le codage de Hamming est parfait lorsqu'il y a égalité dans l'inégalité de la borne de Hamming. On suppose que $r = 1$. Démontrer que le codage de Hamming est parfait si, et seulement si, il existe $k \in \mathbb{N} \setminus \{0; 1\}$ tel que $(p, n) = (2^k - 1 - k, 2^k - 1)$.

Dans le cas où $r = 1$, l'inégalité de la borne de Hamming se réécrit sous la forme

$$2^p \leq \frac{2^n}{1 + n}.$$

Un codage de Hamming parfait est donc caractérisé par l'égalité

$$2^p = \frac{2^n}{1 + n}$$

ou encore

$$n = 2^{n-p} - 1.$$

En posant $k = n - p$, on a donc

$$n = 2^k - 1$$

et, par suite,

$$p = n - k = 2^k - 1 - k.$$

Réiproquement, s'il existe $k \in \mathbb{N}$ tel que $(p, n) = (2^k - 1 - k, 2^k - 1)$, on constate aisément que l'égalité $n = 2^{n-p} - 1$ est satisfaite et que l'on a $p, n \in \mathbb{N}^*$ dès que $k \geq 2$.

En conclusion,

si $r = 1$, le codage de Hamming est parfait si, et seulement si,
il existe $k \in \mathbb{N} \setminus \{0; 1\}$ tel que $(p, n) = (2^k - 1 - k, 2^k - 1)$.

Commentaires :

Pour aller plus loin, on peut essayer de construire des codes de Hamming parfaits.

Pour $r = 1$ et $k = 2$, on a $(p, n) = (1, 3)$. On peut alors prendre pour codage de Hamming l'application Φ de $\mathcal{P}(\{1\})$ vers $\mathcal{P}(\{1, 2, 3\})$ telle que $\Phi(\emptyset) = \emptyset$ et $\Phi(\{1\}) = \{1, 2, 3\}$. En terme binaire, cela revient à coder des messages à 1 bit en messages à 3 bits de la façon suivante : le message 0 est codé par 000 et le message 1 est codé en 111. Si le récepteur reçoit un message dont un bit est altéré, il reçoit ou bien un des messages 001, 010, 100 et il en déduit que le message codé d'origine était 000 (et donc que le bit envoyé est 0) ou bien un des messages 110, 101, 011 et il en déduit que le message codé d'origine était 111 (et donc que le bit envoyé est 1).

Pour $r = 1$ et $k = 3$, on a $(p, n) = (4, 7)$. On peut alors construire le plus classique des codages de Hamming parfaits qui code des messages de 4 bits en messages de 7 bits avec la possibilité de détecter et corriger une erreur de transmission. À ce propos, vous pouvez consulter la page wikipédia [https://fr.wikipedia.org/wiki/Code_de_Hamming_\(7,4\)](https://fr.wikipedia.org/wiki/Code_de_Hamming_(7,4))