Problème

Partie I. Différence symétrique.

1. a. Les propriétés se vérifient immédiatement avec les définitions usuelles. Présentons dans un tableau les traductions comme des propriétés de l'opération Δ.

$(P1)$	$(P2)$	$(P3)$
commutativité	$\emptyset$ est élément neutre	chaque élément est inversible et il est son propre inverse

b. Caractérisons avec les fonctions caractéristiques le fait qu'un x est dans $X \Delta Y$ si et seulement si il appartient à une et une seule des deux parties.

$$x \in X \Delta Y \Leftrightarrow 1_X(x) + 1_Y(x) = 1 \Leftrightarrow 1_X(x) + 1_Y(x) \equiv 1 \mod 2$$

car $1_X(x) + 1_Y(x) \in [\![0, 2]\!]$.

2. a. On utilise les propriétés suivantes (A, B, C sont des parties quelconques de Ω).

$$(1) : A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \qquad (3) : \overline{A \cap B} = \overline{A} \cup \overline{B}$$
$$(2) : A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \qquad (4) : \overline{A \cup B} = \overline{A} \cap \overline{B}$$

$$\begin{aligned}\overline{A \Delta B} = \overline{(A \cap \overline{B}) \cup (\overline{A} \cap B)} &= (\overline{A} \cup B) \cap (A \cup \overline{B}) \text{ d'après (3) et (4)} \\ &= \big((\overline{A} \cup B) \cap A\big) \cup \big((\overline{A} \cup B) \cap \overline{B}\big) \text{ d'après (2)} \\ &= \Big(\underbrace{(\overline{A} \cap A)}_{=\emptyset} \cup (B \cap A)\Big) \cup \Big(\underbrace{(\overline{A} \cap \overline{B})}_{=\emptyset} \cup (B \cap \overline{B})\Big) \text{ d'après (2)} \\ &= (A \cap B) \cup (\overline{A \cup B}) \text{ d'après (4)}\end{aligned}$$

b. On peut utiliser la question a.

$$\begin{aligned}X \Delta (Y \Delta Z) &= \big(X \cap (\overline{Y \Delta Z})\big) \cup \big(\overline{X} \cap (Y \Delta Z)\big) \\ &= \big(X \cap \big((\overline{Y \cup Z}) \cup (Y \cap Z)\big)\big) \cup \big(\overline{X} \cap \big((Y \cap \overline{Z}) \cup (\overline{Y} \cap Z)\big)\big) \\ &= \big(X \cap \overline{Y} \cap \overline{Z}\big) \cup (X \cap Y \cap Z) \cup \big(\overline{X} \cap Y \cap \overline{Z}\big) \cup \big(\overline{X} \cap \overline{Y} \cap Z\big)\end{aligned}$$

Il apparait alors que $X \Delta (Y \Delta Z)$ est constitué des éléments x de Ω appartenant exactement à 1 ou à 3 des parties X, Y, Z.

- $X \cap \overline{Y} \cap \overline{Z}$ est formé par les x appartenant seulement à X et à aucune des deux autres parties. Une situation analogue se produit pour $\overline{X} \cap Y \cap \overline{Z}$ et $\overline{X} \cap \overline{Y} \cap Z$.
- $X \cap Y \cap Z$ est formé par les x appartenant aux trois parties.

Ceci prouve l'associativité de la différence symétrique. En effet Δ est commutative et les trois ensembles jouent des rôles symétriques dans la formulation précédente. Une autre combinaison des parenthèses, comme $(X \Delta Y) \Delta Z$ par exemple, conduira donc au même ensemble d'éléments appartenant à une ou trois des parties données.

c. Notons $\mathcal{P}_p$ la propriété donnée par l'énoncé. Remarquons qu'elle entraine

$$\forall x \in \Omega, \qquad 1_{X_1 \Delta \cdots \Delta X_p}(x) \equiv 1_{X_1}(x) + \cdots + 1_{X_p}(x) \mod 2.$$

Raisonnons par récurrence sur p. La question précédente montre la propriété pour $p = 3$. Montrons l'implication de p à $p+1$.
Considérons des parties $X_1, \cdots, X_{p+1}$, notons $D = X_2 \Delta \cdots \Delta X_{p+1}$.

$$\begin{aligned}x \in X_1 \Delta (X_2 \Delta \cdots \Delta X_{p+1}) &\Leftrightarrow 1_{X_1}(x) + 1_D(x) \equiv 1 \mod 2 \\ &\Leftrightarrow 1_{X_1}(x) + 1_{X_2} + \cdots + 1_{X_p}(x) \equiv 1 \mod 2.\end{aligned}$$

3. a. Par définition de Δ :

$$A \Delta B = \underbrace{(A \cap \overline{B})}_{\subset A} \cup \underbrace{(\overline{A} \cap B)}_{\subset B} \subset A \cup B$$

On « compose » à gauche par A, puis on utilise l'associativité, $(P3)$, $(P2)$

$$\begin{aligned}A \Delta B = \emptyset \Rightarrow A \Delta (A \Delta B) = A \Delta \emptyset \Rightarrow (A \Delta A) \Delta B = A \\ \Rightarrow \emptyset \Delta B = A \Rightarrow B = A\end{aligned}$$

b. D'après l'associativité $(P3)$, $(P2)$:

$$(A \Delta C) \Delta (C \Delta B) = A \Delta \Big(\underbrace{C \Delta C}_{=\emptyset}\Big) \Delta B = A \Delta B$$

On peut injecter ce résultat dans la deuxième expression

$$A \Delta ((A \Delta C) \Delta (C \Delta B)) = A \Delta (A \Delta B) = \Big(\underbrace{A \Delta A}_{=\emptyset}\Big) \Delta B = B$$

4. a. Par définition de la différence symétrique :

$$X_u = \begin{cases} X \cup \{u\} \text{ si } u \notin X \\ X \setminus \{u\} \text{ si } u \in X \end{cases}$$

b. Les formules découlent directement de la description précédente de X_u. Lorsque $u \in B$, la partie $X_u \cap B$ contient un élément de plus ou un élément de moins que la partie $X \cap B$. En revanche, lorsque $u \notin B$, ces deux parties sont égales.

5. a. On peut classer les parties de Ω en deux catégories : celles dont l'intersection avec A est de cardinal pair (les éléments de $\mathcal{P}_A$) et celles dont l'intersection avec A est de cardinal impair (notons $\mathcal{I}$ l'ensemble qu'elles constituent). On a évidemment

$$\sharp\mathcal{P}_A + \sharp\mathcal{I} = \sharp\mathcal{P}(\Omega) = 2^n$$

Comme A est non vide, on peut considérer un $u \in A$ et l'application

$$\begin{cases} \mathcal{P}(\Omega) \to \mathcal{P}(\Omega) \\ X \to X_u \end{cases}$$

Elle est involutive d'après les propriétés de Δ et définit une bijection de $\mathcal{P}_A$ vers $\mathcal{I}$ d'après 4.b.. Ces deux ensembles ont donc le même nombre d'éléments qui est la moitié de 2^n soit 2^{n-1}.

b. Remarquons d'abord que comme A_1 et A_2 sont distinctes, il existe un élément appartenant à l'un et pas à l'autre : par exemple un u appartenant à A_2 et n'appartenant pas à A_1. Cet élément u sera utilisé dans la suite.
Le raisonnement est alors proche du précédent. On classe les éléments de $\mathcal{P}_{A_1}$ en deux catégories suivant la parité du cardinal de l'intersection avec A_2. Celle attachée aux impairs est l'ensemble $\mathcal{P}_{A_1} \cap \mathcal{P}_{A_2}$ qui nous intéresse.
L'involution $X \to X_u$ définit une bijection entre les deux catégories. Elle conserve la parité de l'intersection avec A_1 car $u \notin A_1$ mais change l'autre. Les deux catégories ont donc le même nombre d'éléments 2^{n-2}.

c. Le raisonnement est le même que lors des questions précédentes en utilisant un u qui est dans A_3 mais ni dans A_1 ni dans A_2. Il en existe car A_3 n'est pas inclus dans $A_1 \cup A_2$. On peut construire une involution entre les deux catégories d'éléments de $P_{A_1} \cap \mathcal{P}_{A_2}$ définies par la parité du cardinal de l'intersection avec A_3.
La condition $A_3 \not\subset A_1 \cup A_2$ n'est sans doute pas la meilleure mais elle suffit pour la suite. Une condition plus satisfaisante ferait intervenir des différences symétriques.

Partie II. Distance de Hamming.

1. Si $d(A,B) = 0$ alors $\sharp(A \,\Delta\, B) = 0$ c'est à dire $A \,\Delta\, B = \emptyset$. D'après I.3.a. ceci entraîne $A = B$.

2. Soient A, B, C trois parties quelconques de Ω. D'après I.3.b. :

$$(A \,\Delta\, C) \,\Delta\, (C \,\Delta\, B) = A \,\Delta\, B$$

On en déduit :

$$d(A,B) = \sharp(A \,\Delta\, B) = \sharp\left((A \,\Delta\, C) \,\Delta\, (C \,\Delta\, B)\right) \leq \sharp(A \,\Delta\, C) + \sharp(C \,\Delta\, B)$$

car $X \,\Delta\, Y \subset X \cup Y$. Ce qui donne l'inégalité triangulaire

$$d(A,B) \leq d(A,C) + d(C,B)$$

Cette inégalité permet de récupérer un peu d'intuition géométrique pour la suite.

3. Désignons par $\mathcal{P}_k(\Omega)$ l'ensemble des parties à k éléments de Ω. L'application

$$\begin{cases} \mathcal{S}(C,k) \to \mathcal{P}_k(\Omega) \\ X \to C \,\Delta\, X \end{cases}$$

est une bijection entre la sphère et l'ensemble des parties car $C \,\Delta\, X = Y$ si et seulement si $X = C \,\Delta\, Y$ (involution). On en déduit (en notant $n = \sharp\Omega$)

$$\sharp S(C,k) = \binom{n}{k}$$

Une boule de rayon k est l'union des shères de rayon $0, 1, \cdots, k$ d'où

$$\sharp\mathcal{B}(C,k) = \underset{\substack{\uparrow \\ \text{rayon } 0}}{1} + \underset{\substack{\uparrow \\ \text{rayon } 1}}{n} + \binom{n}{2} + \cdots + \binom{n}{k} = \sum_{i=0}^{k} \binom{n}{i}$$

Partie III. Communiquer sûrement c'est organiser le délayage.

1. La propriété $k \geq 0$ caractérise l'injectivité de la fonction Φ. En effet, $\Phi(X) = \Phi(Y)$ si et seulement si $d(\Phi(X), \Phi(Y)) = 0$.

2. Dans cette question, k est un entier pair non nul. Supposons que l'intersection des deux boules ne soit pas vide et notons Z un élément de cette intersection. Utilisons l'inégalité triangulaire :

$$\left.\begin{aligned} d(\Phi(X), Z) &\leq \frac{k}{2} \\ d(\Phi(Y), Z) &\leq \frac{k}{2} \end{aligned}\right\} \Rightarrow d(\Phi(X), \Phi(Y)) \leq d(\Phi(X), Z) + d(Z, \Phi(Y)) \leq k$$

en contradiction avec la propriété fondamentale de Φ qui est que deux images sont « k-loin ». Les boules sont donc disjointes.

3. a. Ici $k = 2$. Les boules $\mathcal{B}(\Phi(X), 1)$ centrées aux images sont deux à deux disjointes d'après la question précédente. Il y en a autant que de parties dans E c'est à dire 2^p. Chaque boule contient $n+1$ éléments d'après II.3. La réunion de ces boules est une partie de $\mathcal{P}(F)$. On en déduit :

$$2^p(n+1) \leq 2^n \Rightarrow n+1 \leq 2^{n-p}$$

Le tableau

n	5	6	7
$n+1$	6	7	8
2^{n-p}	2	4	8

montre que la plus petite valeur possible pour n est 7. La partie IV. donne un exemple de fonction Φ vérifiant ces conditions.

b. Ici $k = 4$. Cette fois, les boules de rayon 2 sont deux à eux disjointes. Le nombre de ces boules est toujours 2^p et chaque boule contient

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

La réunion de ces boules disjointes est une partie de $\mathcal{P}(\Omega)$ donc

$$\frac{1}{2}(n^2 + n + 2)2^p \leq 2^n \Rightarrow n^2 + n + 2 \leq 2^{n-p+1}$$

Lorsque $p = 4$, pour trouver la plus petite valeur de n pour laquelle cette inégalité est possible, on forme un tableau analogue au précédent :

n	5	6	7	8	9	10
n^2+n+2	32	44	58	74	92	112
2^{n-p+1}	4	8	16	32	64	128

On en déduit que la plus petite valeur pour laquelle un délayage avec $k = 4$ est possible est 10.

Partie IV. Code de Hamming.

1. Comme 0 est un nombre pair, aucun des p_i n'est dans $\Phi(\emptyset)$ donc $\Phi(\emptyset) = \emptyset$.
Chaque intersection de E avec les A_i contient trois éléments. Les trois p_i sont donc dans $\Phi(E)$ et $\Phi(E) = F$.
Par des raisonnements analogues, on trouve

$$\Phi(\{d_1\}) = \{d_1, p_1, p_2\}, \quad \Phi(\{d_1, d_2, d_4\}) = \{d_1, d_2, d_4, p_1\}$$

2. Pour i entre 1 et 3, le seul élément de $A_i \cap (F \setminus E)$ est p_i. Pour tout élément X de $\mathcal{P}(E)$, on a donc (par définition de Φ) :

$$A_i \cap \Phi(X) = \begin{cases} (A_i \cap X) & \text{si } \sharp(A_i \cap X) \text{ est pair} \\ (A_i \cap X) \cup \{p_i\} & \text{si } \sharp(A_i \cap X) \text{ est impair} \end{cases}$$

On en déduit que $\sharp(A_i \cap \Phi(X))$ est toujours pair.

3. Il est difficile de rédiger une argumentation globale permettant de montrer le résultat demandé. On se contentera d'examiner toutes les parties Z de F non vides et de cardinal 1 ou 2 et de préciser pour chacune un A_i tel que $\sharp(A_i \cap Z)$ soit un singleton. Les résultats sont présentés avec des tableaux regroupant les $7 + \binom{7}{2} = 28$ parties Z en diverses catégories :
   - les singletons. Il y en a 7.
   - les paires d'éléments de E. Il y en a 6.
   - les paires d'éléments de $F \setminus E$. Il y en a 3.
   - les paires avec un élément dans E et un dans $F \setminus E$. Il y en a $4 \times 3 = 12$, on les présente en trois tableaux de quatre.

$\{d_1\}$	$\{d_2\}$	$\{d_3\}$	$\{d_4\}$	$\{p_1\}$	$\{p_2\}$	$\{p_4\}$
A_1	A_1	A_2	A_1	A_1	A_2	A_3

$\{d_1, d_2\}$	$\{d_1, d_3\}$	$\{d_1, d_4\}$	$\{d_2, d_3\}$	$\{d_2, d_4\}$	$\{d_3, d_4\}$
A_2	A_1	A_2	A_1	A_2	A_1

$\{p_2, p_3\}$	$\{p_1, p_3\}$	$\{p_1, p_2\}$
A_2	A_1	A_1

$\{d_1, p_1\}$	$\{d_2, p_1\}$	$\{d_3, p_1\}$	$\{d_4, p_1\}$
A_2	A_3	A_1	A_2

$\{d_1, p_2\}$	$\{d_2, p_2\}$	$\{d_3, p_2\}$	$\{d_4, p_2\}$
A_1	A_1	A_4	A_1

$\{d_1, p_3\}$	$\{d_2, p_3\}$	$\{d_3, p_3\}$	$\{d_4, p_3\}$
A_1	A_1	A_2	A_1

4. Lorsque des parties sont disjointes, le nombre d'éléments de l'union est la somme des

cardinaux. C'est le cas pour :

$$\begin{aligned} A \cap (U \,\Delta\, V) &= \left(A \cap U \cap \overline{V}\right) \cup \left(A \cap \overline{U} \cap V\right) \\ A \cap U &= (A \cap U \cap V) \cup \left(A \cap U \cap \overline{V}\right) \\ A \cap V &= (A \cap U \cap V) \cup \left(A \cap \overline{U} \cap V\right) \end{aligned}$$

On en déduit des égalités entre nombres d'éléments. On les somme et on prend le reste modulo 2 :

$$\begin{aligned} \sharp(A \cap U) &= \sharp\left(A \cap U \cap V\right) + \sharp\left(A \cap U \cap \overline{V}\right) \\ \sharp(A \cap V) &= \sharp\left(A \cap U \cap V\right) + \sharp\left(A \cap \overline{U} \cap V\right) \\ \sharp(A \cap U) + \sharp(A \cap V) &\equiv \sharp\left(A \cap (U \,\Delta\, V)\right) \mod 2 \end{aligned}$$

Comme $\sharp(A \cap V) \equiv -\sharp(A \cap V) \mod 2$, on obtient bien la relation annoncée :

$$\sharp(A \cap U) - \sharp(A \cap V) \equiv \sharp\left(A \cap (U \,\Delta\, V)\right) \mod 2$$

5. Soient X et Y des parties de E distinctes. On veut montrer que $d(\Phi(X), \Phi(Y)) > 2$.
Il est clair que $\Phi(X)$ et $\Phi(Y)$ sont distinctes car $\Phi(X) \cap E = X$ entraîne que Φ est injective. Mais notre objectif est plus difficile.
D'après la question 2., pour tout i entre 1 et 3, $\sharp\left(A_i \cap \Phi(X)\right)$ et $\sharp\left(A_i \cap \Phi(Y)\right)$ sont pairs. Ceci entraîne d'après la question 4 que

$$\sharp\left(A_i \cap (\Phi(X) \,\Delta\, \Phi(Y))\right) \equiv 0 \mod 2$$

Notons $Z = \Phi(X) \,\Delta\, \Phi(Y)$. On a donc :

$$\forall i \in \{1, 2, 3\} : \sharp(A_i \cap Z) \equiv 0 \mod 2$$

Or d'après 3., si Z est non vide et de cardinal inférieur ou égal à 2, il existe un A_i tel que $\sharp(A_i \cap Z) = 1$. On en déduit donc que

$$d(\Phi(X), \Phi(Y)) = \sharp(\Phi(X) \,\Delta\, \Phi(Y)) > 2$$

6. Avec les notations de I.5., il s'agit de montrer que

$$\{\Phi(X),\ X \in \mathcal{P}(E)\} = \mathcal{P}_{A_1} \cap \mathcal{P}_{A_2} \cap \mathcal{P}_{A_2}.$$

Or A_1, A_2, A_3 vérifient les conditions de I.5.c donc

$$\sharp\left(\mathcal{P}_{A_1} \cap \mathcal{P}_{A_2} \cap \mathcal{P}_{A_2}\right) = 2^{n-3} = 2^4$$

c'est à dire le même que celui de l'ensemble des images. Comme la question IV.4. a montré l'inclusion de l'ensemble des images dans l'intersection des $\mathcal{P}_{A_i}$, on a bien prouvé l'égalité demandée.
Pour continuer cette étude, il vaut mieux se placer dans le cadre des espaces vectoriels de dimension finie sur le corps à deux éléments.