Ce devoir en 4 heures comprend en plus de ce problème une partie algorthmique (1h30) sur la représentation de Zeckendorf.

L'objectif de ce problème est de présenter dans un cadre ensembliste la *distance de Hamming* ainsi qu'un exemple de *code de Hamming*[1].

Pour tout ensemble fini E, on notera $\sharp E$ son cardinal (nombre d'éléments).

Partie I. Différence symétrique.

Dans cette partie Ω désigne un ensemble fini. Pour toute partie X de Ω, le complémentaire de X dans Ω est noté $\overline{X}$ et la fonction caractéristique de X est notée 1_X.

$$\forall x \in \Omega,\ 1_X(x) = \begin{cases} 1 \text{ si } x \in X \\ 0 \text{ sinon} \end{cases}$$

On définit dans $\mathcal{P}(\Omega)$ une opération (notée Δ) appelée *différence symétrique* par :

$$\forall (X,Y) \in \mathcal{P}(\Omega) \times \mathcal{P}(\Omega) : X \,\Delta\, Y = (\overline{X} \cap Y) \cup (X \cap \overline{Y})$$

1. a. Vérifier les propriétés suivantes et les traduire dans le vocabulaire des opérations :

$$\begin{array}{lrr} (P1) & \forall (X,Y) \in \mathcal{P}(\Omega) \times \mathcal{P}(\Omega) : & X \,\Delta\, Y = Y \,\Delta\, X \\ (P2) & \forall X \in \mathcal{P}(\Omega) : & X \,\Delta\, \emptyset = \emptyset \,\Delta\, X = X \\ (P3) & \forall X \in \mathcal{P}(\Omega) : & X \,\Delta\, X = \emptyset \end{array}$$

b. Montrer que :

$$\forall (X,Y) \in \mathcal{P}(\Omega)^2, \forall x \in \Omega, \quad x \in X \,\Delta\, Y \Leftrightarrow 1_X(x) + 1_Y(x) \equiv 1 \mod 2.$$

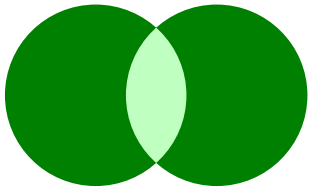

FIG. 1: Différence symétrique

[1] d'après http ://fr.wikipedia.org/wiki/Code_de_Hamming

2. a. Montrer que

$$\forall (X,Y) \in \mathcal{P}(\Omega) \times \mathcal{P}(\Omega) : \overline{X \,\Delta\, Y} = \left(\overline{X \cup Y}\right) \cup (X \cap Y)$$

b. Soient X, Y, Z trois parties de Ω. Exprimer $X \,\Delta (Y \,\Delta\, Z)$ comme une union de parties deux à deux disjointes, chacune de ces parties étant une intersection de trois. En déduire l'associativité de Δ.

c. Soient $X_1, X_2, \cdots, X_p$ des parties de Ω et x un élément de Ω. Montrer que

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

Comme Δ est associative, il est inutile d'écrire des parenthèses dans $X_1 \,\Delta \cdots \Delta\, X_p$.

3. Dans cette question A, B, C sont des parties quelconques de Ω.

a. Montrer que $A \,\Delta\, B \subset A \cup B$ et que :

$$A \,\Delta\, B = \emptyset \Rightarrow A = B$$

b. Simplifier $(A \,\Delta\, C) \,\Delta\, (C \,\Delta\, B)$ et $A \,\Delta\, ((A \,\Delta\, C) \,\Delta\, (C \,\Delta\, B))$.

4. Pour tout élément $u \in \Omega$ et toute partie X de Ω, on note $X_u = \{u\} \,\Delta\, X$.

a. Préciser X_u.

b. Soit B une partie quelconque de Ω. Montrer que :

$$\sharp(X_u \cap B) \equiv \begin{cases} \sharp(X \cap B) + 1 \text{ si} & u \in B \\ \sharp(X \cap B) \text{ si} & u \notin B \end{cases} \mod 2.$$

5. Ici Ω contient n éléments. Pour tout $A \subset \Omega$, on désigne par $\mathcal{P}_A$ l'ensemble des parties X de Ω telles que

$$\sharp(X \cap A) \equiv 0 \mod 2$$

a. Montrer que $\sharp \mathcal{P}_A = 2^{n-1}$ lorsque A est non vide.

b. Soient A_1 et A_2 deux parties non vides et distinctes de Ω. Montrer que

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

c. Soient A_1 et A_2 A_3 trois parties non vides, deux à deux distinctes de Ω. On suppose de plus que A_3 n'est pas incluse dans $A_1 \cup A_2$. Montrer que

$$\sharp\left(\mathcal{P}_{A_1} \cap \mathcal{P}_{A_2} \cap \mathcal{P}_{A_3}\right) = 2^{n-3}$$

Partie II. Distance de Hamming.

On reprend les notations de la section précédente et on définit la *distance de Hamming* $d(X,Y)$ entre deux parties X et Y de Ω par

$$\forall (X,Y) \in \mathcal{P}(\Omega)\times\mathcal{P}(\Omega) : d(X,Y) = \sharp(X \,\Delta\, Y).$$

1. Montrer que $d(A,B)=0$ entraîne $A=B$ pour toutes parties A et B de Ω.
2. Montrer l'inégalité triangulaire :
$$\forall (A,B,C) \in (\mathcal{P}(\Omega))^3 : d(A,B) \leq d(A,C)+d(C,B)$$
3. Soit $C \subset \Omega$ et $k \in \mathbb{N}$, on définit la *H-sphère* de centre C et de rayon k (notée $\mathcal{S}(C,k)$) et la *H-boule* de centre C et de rayon k (notée $\mathcal{B}(C,k)$) par :
$$\forall X \in \mathcal{P}(\Omega), \quad \begin{cases} X \in \mathcal{S}(C,k) \Leftrightarrow & d(C,X)=k \\ X \in \mathcal{B}(C,k) \Leftrightarrow & d(C,X)\leq k \end{cases}$$
On note n le nombre d'éléments de Ω. Quel est le nombre d'éléments d'une sphère de rayon k ? Quel est le nombre d'éléments d'une boule de rayon k ?

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

Dans cette partie E désigne un ensemble à p éléments. On imagine un système de transmission qui « émet » des parties X de E vers un récepteur. Mais de petites erreurs peuvent survenir lors de la transmission et de temps en temps le X reçu n'est pas tout à fait le X émis. Pour remédier à cela, on va transformer (coder) le X en $\Phi(X)$ de sorte que chaque $\Phi(X)$ soit « isolé » puis transmettre le $\Phi(X)$. Si une petite erreur survient lors de la transmission, le récepteur saura la repérer et éventuellement la corriger ou demander une nouvelle émission. Il devra ensuite décoder le $\phi(X)$ en X.
On suppose donc l'existence d'un ensemble F à n éléments contenant E, de $k \in \mathbb{N}$ et d'une application Φ de $\mathcal{P}(E)$ dans $\mathcal{P}(F)$ telle que :

$$\forall (X,Y) \in \mathcal{P}(E), \qquad X \neq Y \Rightarrow d(\Phi(X),\Phi(Y)) > k$$

où d désigne la distance de Hamming dans $\mathcal{P}(F)$.

1. Que signifie pour Φ le fait que k soit supérieur ou égal à 0 ?
2. On suppose k non nul et pair. Montrer que :
$$\forall (X,Y) \in \mathcal{P}(E)^2, \qquad X \neq Y \Rightarrow \mathcal{B}(\Phi(X),\frac{k}{2}) \cap \mathcal{B}(\Phi(Y),\frac{k}{2}) = \emptyset$$
3. a. On suppose $k=2$. Montrer que $n+1 \leq 2^{n-p}$. Quelle est la plus petite valeur possible pour n si $p=4$?
   b. On suppose $k=4$. Former une inégalité que doivent vérifier p et n. Quelle est la plus petite valeur possible pour n si $p=4$?

Partie IV. Code de Hamming.

L'objet de cette section est de donner un exemple de fonction Φ vérifiant les propriétés de la section III. Ici, E est un ensemble à 4 éléments et F est un ensemble à 7 éléments contenant E. On note

$$E=\{d_1,d_2,d_3,d_4\} \qquad F=\{d_1,d_2,d_3,d_4,p_1,p_2,p_3\}$$

Certaines parties de F, notées A_1, A_2, A_3, vont jouer un rôle particulier :

$$A_1=\{d_1,d_2,d_4,p_1\} \qquad A_2=\{d_1,d_3,d_4,p_2\} \qquad A_3=\{d_2,d_3,d_4,p_3\}$$

On définit une fonction ϕ de $\mathcal{P}(E)$ dans $\mathcal{P}(F)$ la manière suivante.

$$\forall X \in \mathcal{P}(E), \Phi(X) \text{ défini par } : \begin{cases} \Phi(X) \cap E = X \\ p_1 \in \Phi(X) \Leftrightarrow \sharp(X \cap \{d_1,d_2,d_4\}) \text{ impair} \\ p_2 \in \Phi(X) \Leftrightarrow \sharp(X \cap \{d_1,d_3,d_4\}) \text{ impair} \\ p_3 \in \Phi(X) \Leftrightarrow \sharp(X \cap \{d_2,d_3,d_4\}) \text{ impair} \end{cases}$$

1. Calculer $\Phi(\emptyset)$, $\Phi(E)$, $\Phi(\{d_1\})$, $\Phi(\{d_1,d_2,d_4\})$.
2. Montrer que, pour toute partie X de E et tout entier i entre 1 et 3, $A_i \cap \Phi(X)$ contient un nombre pair d'éléments.
3. Montrer que, pour toute partie non vide Z de F :
$$\sharp Z \leq 2 \Rightarrow \exists i \in \{1,2,3\} \text{ tel que } \sharp(A_i \cap Z) = 1$$
4. Soient A, U, V des parties quelconques de F, montrer que
$$\sharp(A \cap U) - \sharp(A \cap V) \equiv \sharp(A \cap (U \,\Delta\, V)) \mod 2$$
5. Montrer que pour toutes parties (de E) X et Y distinctes , la distance de Hamming entre $\Phi(X)$ et $\Phi(Y)$ est strictement plus grande que 2.
6. (hors barême)[2] Soit Z une partie de F. Montrer qu'il existe une partie X de E telle que $Z=\Phi(X)$ si et seulement si $\sharp(A_1 \cap Z)$, $\sharp(A_2 \cap Z)$, $\sharp(A_3 \cap Z)$ sont pairs.

[2] pour aller plus loin, il est bien plus commode d'utiliser la présentation classique des codes correcteurs à base d'algèbre linéaire sur le corps à deux éléments

Rémy Nicolai S0904E