Codes correcteurs

partie 1

Odile PAPINI, SIS. Université de Toulon et du Var, Toulon.
papini@univ-tln.fr

Plan

- Bases mathématiques
  - **théorie des ensembles**
  - **algèbre linéaire**
  - **corps finis**
  - **probabilités**
  - **théorie de l'information**
  - **complexité**

- Codes correcteurs
  - **introduction historique**
  - **généralités**
  - **codes linéaires**

Théorie des ensembles

ensemble : liste ou collection d'objets

élément : objet appartenant à l'ensemble

$p \in A$ si p est un élément de l'ensemble A

A et B des ensembles

A **est sous-ensemble de** B **:** si tout élément de A est élément de B

$$A \subset B$$

$A = B$ si et seulement si $A \subset B$ et $B \subset A$

ensemble vide : $\emptyset$

ensemble universel : U

exemples : $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$, $\cdots$

Opérations sur les ensembles

A et B des ensembles

$$A \cup B = \{x,\ x \in A \text{ ou } x \in B\}$$

$$A \cap B = \{x,\ x \in A \text{ et } x \in B\}$$

$$C_A B = \{x,\ x \in A \text{ et } x \notin B\}$$

propriétés

idempotence $A \cup A = A$ $A \cap A = A$

associativité $(A \cup B) \cup C = A \cup (B \cup C)$ $(A \cap B) \cap C = A \cap (B \cap C)$

commutativité $A \cup B = B \cup A$ $A \cap B = B \cap A$

distributivité $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

identité $A \cup \emptyset = A \quad A \cap U = A \quad A \cup U = U \quad A \cap \emptyset = \emptyset$

complémentarité $A \cup CA = U \quad A \cap CA = \emptyset \quad CCA = A$

$CU = \emptyset \quad C\emptyset = U$

lois de Morgan $C(A \cup B) = CA \cap CB \quad C(A \cap B) = CA \cup CB$

fonctions et applications

fonction de E vers F : une correspondance entre un élément de E et un élément de F (chaque élément de E a au plus un correspondant dans F)

application : fonction de E vers F (chaque élément de E a exactement un correspondant dans F)

f fonction de E vers F

fonction injective : $\forall x_1 \in E,\ \forall x_2 \in E \quad si \quad f(x_1) = f(x_2) \quad alors \quad x_1 = x_2$

fonction surjective : $\forall y \in F,\ \exists x \in E \quad tq \quad y = f(x)$

fonction bijective : f est injective et surjective

ensembles finis

Un ensemble E est **fini** : s'il existe une bijection de E dans un ensemble de la forme $\{i \in \mathbb{N},\ tq\ 1 \leq i \leq n\}, n \in \mathbb{N}$

Un ensemble E est **fini** si toute application injective de E dans E est surjective

Soit E un ensemble fini et f une application de E dans E les 3 conditions sont équivalentes :

- f est injective
- f est surjective
- f est bijective

$card(E)$: **cardinal** d'un ensemble fini i.e. le nombre d'éléments d'un ensemble E

Soit E un ensemble fini et F un sous-ensemble de E alors F est fini et

$$card(F) \leq card(E)$$

Soit E et F des ensembles finis :

$card(E) \leq card(F)$ ssi il existe une **application injective** de E vers F

$card(E) \geq card(F)$ ssi il existe une **application surjective** de E vers F

$card(E) = card(F)$ ssi il existe une **application bijective** de E vers F

$card(E \cup F) = card(E) + card(F) - card(E \cap F)$

$card(E \times F) = card(E)\ card(F)$

si $(E_i)_{i \in I}$ est une **partition de** E alors $card(E) = \Sigma_{i \in I}\ card(E_i)$

nombre d'applications d'un ensemble E fini vers un ensemble F fini : $card(F)^{card(E)}$

nombre de parties d'un ensemble E : $2^{card(E)}$

Dénombrement

factorielle : produit des entiers positifs de 1 à n

$$n! = 1\ 2\ 3\ \cdots\ (n-2)\ (n-1)\ n \qquad 0! = 1$$

Soit E un ensemble fini, $card(E) = n$ et $[k] = \{j \in \mathbb{N},\ 1 \leq j \leq k\}$

arrangement : nombre des applications injectives de $[k]$ dans E

$$A_n^k = \frac{n!}{(n-k)!}$$

permutation : nombre des applications bijectives de E dans E

$$P_n = n!$$

combinaison : nombre de sous-ensembles de E de cardinal k

$$C_n^k = \frac{n!}{k!(n-k)!}$$

Coefficients du binôme

$$C_n^k \;=\; 0 \quad \text{pour } k > n \leq 0$$

$$C_n^{n-k} \;=\; C_n^k$$

$$C_{n+1}^k \;=\; C_n^{k-1} + C_n^k$$

$$\Sigma_{k=0}^n \, C_n^k \;=\; 2^n$$

$$\Sigma_{k\ pair} \, C_n^k \;=\; \Sigma_{k\ impair} \, C_n^k = 2^{n-1} \quad \text{avec } n \geq 1$$

$$(x+y)^n \;=\; \Sigma_{k=0}^n \, C_n^k \, x^{n-k} \, y^k$$

groupes

loi interne $\star$ dans un ensemble E : application de $E \times E$ dans E

$$(x, y) \to x \star y$$

structure $(E, \star)$: E un ensemble et $\star$ loi interne

groupe $(G, \star)$: une structure telle que

- $\forall x \in G,\ \forall y \in G,\ \forall z \in G, \quad x \star (y \star z) = (x \star y) \star z)$ **associativité**
- $\exists e \in G,\ tq\ \forall x \in G, \quad x \star e = e \star x = x$ **élément neutre**
- $\forall x \in G,\ \exists x',\ tq \quad x \star x' = x' \star x = e$ **élément symétrique**

$(G, \star)$ est un groupe **commutatif** si $\quad \forall x \in G, \forall y \in G, \quad x \star y = y \star x$

sous-groupes

un sous-ensemble non vide H de G est **stable** si

$$\forall x \in H,\ \forall y \in H, \quad x \star y \in H$$

un sous-ensemble H de G est un **sous-groupe** de G ssi

- H est stable
- $e \in H$
- $\forall x \in H,\ x' \in H$, (x' symétrique de x)

un **morphisme** de $(E, \star)$ dans $(F, \perp)$ est une application f de E vers F tq :

$$\forall x \in E,\ \forall y \in E \quad f(x \star y) = f(x) \perp f(y)$$

si f est **bijective** alors f est un **isomorphisme**

anneau

anneau $(A, \star, \perp)$: une structure telle que

- $(A, \star)$ est un sous-groupe commutatif
- $\forall x \in A,\ \forall y \in A,\ \forall z \in A, \quad x \perp (y \perp z) = (x \perp y) \perp z)$ **associativité**
- $\forall x \in A,\ \forall y \in A,\ \forall z \in A, \quad x \perp (y \star z) = (x \perp y) \star (x \perp z)$ **distributivité à gauche**
- $\forall x \in A,\ \forall y \in A,\ \forall z \in A, \quad (x \star y) \perp z = (x \perp z) \star (y \perp z)$ **distributivité à droite**
- $\exists\, 1 \in A,\ tq\ \forall x \in A, \quad x \perp 1 = 1 \perp x = x$ **élément unité**

$(A, \star, \perp)$ est un anneau **commutatif** si $\quad \forall x \in G, \forall y \in A, \quad x \perp y = y \perp x$

$(A, \star, \perp)$ est un **corps** si tout élément de $A \backslash \{0\}$ possède un symétrique

espace vectoriel

loi externe $\times$ entre éléments de K et de E : application de $K \times E$ dans E

$$(x, y) \to x \times y$$

espace vectoriel $(E, +, \times)$ sur K corps commutatif : une structure telle que

- $(E, +)$ est un groupe commutatif
- $\forall \lambda \in K,\ \forall \mu \in K\ , \forall x \in E, \quad \lambda(\mu \times x) = (\lambda\mu) \times x$
- $e \in K$ élément neutre $\quad e \times x = x$
- $\forall \lambda \in K,\ \forall \mu \in K,\ \forall x \in E, \quad (\lambda + \mu) \times x = \lambda x + \mu x$
- $\forall \lambda \in K,\ \forall x \in E,\ \forall y \in E, \quad \lambda(x + y) = \lambda x + \lambda y$

sous-espace vectoriel

F **sous-espace vectoriel** de E sur K :

- F non vide
- stable pour $+$
- stable pour $\times$

F est un **sous-espace vectoriel** de E sur K ssi

- F non vide
- $\forall x \in F,\ \forall y \in F \quad x - y \in F$
- $\forall x \in F,\ \forall \lambda \in K \quad \lambda \times x \in F$

base

$A = \{x_1, x_2, \cdots, x_p\}$ est une partie **génératrice** d'un s. e. v., F sur K :

si F est le sous-espace vectoriel des combinaisons linéaires de $x_1, x_2, \cdots, x_p$

$A = \{x_1, x_2, \cdots, x_p\}$ est une partie **libre** d'un s. e. v. F sur K si

$$(\lambda_i \in K)\ i \in [1, p] \quad \text{si} \quad \Sigma_{i=1}^{p}\ \lambda_i \times x_i = 0 \quad \text{alors} \quad \lambda_i = 0,\ \forall i \in [1, p]$$

une **base** d'un s. e. v. est une partie **libre** et **génératrice**

la **dimension** d'un s. e. v. est nombre d'eĺéments d'une de ses bases

morphismes d'espaces vectoriels

morphisme d'espaces vectoriels :

f fonction de E dans E', espaces vectoriels sur K

- $\forall x \in E, \forall y \in E \quad f(x+y) = f(x) + f(y)$
- $\forall x \in E, \forall \lambda \in K \quad f(\lambda \times x) = \lambda \times f(x)$

f bijective **isomorphisme** de E sur E'

f bijective et $E = E'$ **automorphisme** sur E

application linéaire

soit E et E' des espaces vectoriels sur K **application linéaire** fonction de E vers E' telle que

- $\forall x \in E, \forall y \in E \quad f(x+y) = f(x) + f(y)$
- $\forall x \in E, \forall \lambda \in K \quad f(\lambda \times x) = \lambda \times f(x)$

image d'une application linéaire f : $Imf = \{y \in E',\ y = f(x), \forall x \in E\}$

noyau d'une application linéaire f : $Kerf = \{x \in E,\ f(x) = 0\}$

rang d'une application linéaire f : $rang(f) = dim(E) - dim(Kerf)$

Théorie des probabilités

ensemble fondamental S : ensemble de tous les résultats possibles d'une expérience

évènement A : ensemble de résultats, $A \subseteq S$

évènement **élémentaire** : $A = \{a\}, \quad a \in S$

évènement **impossible** : $\emptyset$

évènement **certain** : S

combinaisons dévènements :

- $A \cup B$: évènement qui se produit si A **ou** B **est réalisé**
- $A \cap B$: évènement qui se produit si A **et** B **sont réalisés**
- CA : évènement qui se produit si A **n'est pas réalisé**

Axiomes du calcul des probabilités

S : ensemble fondamental, ϵ : famille d'évènements, $P : \epsilon \quad \to \mathbb{R}$

$P_1)$ pour tout A, $\quad 0 \leq P(A) \leq 1$

$P_2)$ $\quad P(S) = 1$

$P_3)$ si $\quad A \cap B = \emptyset \quad$ alors $\quad P(A \cup B) = P(A) + P(B)$

Théorèmes

- $P(\emptyset) = 0$
- $P(C_A) = 1 - P(A)$
- si $A \subset B \quad$ alors $\quad P(A) \leq P(B)$
- $P(C_A B) = P(A) - P(A \cap B)$
- $P(A \cup B) = P(A) + P(B) - P(A \cap B)$

ensemble probabilisé fini

ensemble fondamental **fini** $S = \{a_1, a_2, \cdots, a_n\}$

$p_i \in \mathbb{R}$: **probabilité** de a_i tq

- $p_i \geq 0$
- $\Sigma_{i=1}^{n}\ p_i = 1$

$A = \{a_1, a_2, \cdots, a_k\}$, $k < n$, probabilité d'un évènement A

$$P(A) = \Sigma_{i=1}^{k}\ P(a_i)$$

ensembles équiprobables finis

ensemble fondamental S : ensemble fini $S = \{a_1, a_2, \cdots, a_n\}$

$\forall i \in \{1, n\},\ P(a_i) = \frac{1}{n}$

évènement A : $S = \{a_1, a_2, \cdots, a_r\}$

$P(A) = \frac{r}{n}$

$$P(A) = \frac{nombre\ de\ cas\ favorables\ à\ la\ réalisation\ de\ A}{nombre\ de\ cas\ possibles\ de\ l'ensemble\ fondamental\ S}$$

exemple : tirage d'une carte dans un jeu de 52 cartes

$A = \{$ la carte est un pique $\}$ $\qquad$ $P(A)$?

$B = \{$ la carte est une tête $\}$ $\qquad$ $P(B)$? $\qquad$ $P(A \cap B)$?

probabilité conditionnelle

B évènement, $P(B) > 0$

$$P(A|B) = \frac{P(A \cap B)}{P(B)}$$

S équiprobable fini :

$$P(A \cap B) = \frac{card(A \cap B)}{card(S)}, \quad p(B) = \frac{card(B)}{card(S)}$$

$$P(A|B) = \frac{P(A \cap B)}{P(B)} = \frac{card(A \cap B)}{card(B)}$$

$$P(A|B) = \frac{nombre\ de\ réalisations\ possibles\ de\ A}{nombre\ de\ réalisations\ possibles\ de\ B}$$

théorème de Bayes

ensemble fondamental S : ensemble fini, $S = A_1 \cup A_2 \cup \cdots \cup A_n$
$A_1, A_2, \cdots A_n$ partition de S

$$B = S \cap B = (A_1 \cup A_2 \cup A_n) \cap B = (A_1 \cap B) \cup (A_2 \cap B) \cup \cdots \cup (A_n \cap B)$$

$$P(B) = P(A_1 \cap B) + P(A_2 \cap B) + \cdots + P(A_n \cap B)$$

$$P(B) = P(A_1)P(B|A_1) + P(A_2)P(B|A_2) + \cdots + P(A_n)P(B|A_n)$$

$$P(A_i|B) = \frac{P(A_i \cap B)}{P(B)}$$

Théorème de Bayes :

$$P(A_i|B) = \frac{P(A_i)P(B|A_i)}{P(A_1)P(B|A_1) + P(A_2)P(B|A_2) + \cdots + P(A_n)P(B|A_n)}$$