Réseaux, information et communications (INFO-F303)
Partie Théorie de l'Information
Rappels mathématiques

Christophe Petit

Université libre de Bruxelles

Plan du cours

1. Notion de code
2. Source aléatoire et codes efficaces
3. Entropie et codage efficace
4. Compression sans perte
5. Canal bruité
6. Codes correcteurs d'erreurs
7. Codes linéaires
8. Quelques familles de codes linéaires

A. Rappels mathématiques (chapitre 7.1 du syllabus)

Groupe

- Un groupe $(G, \circ)$ est un ensemble G muni d'une opération $\circ : G \times G \rightarrow G$ telle que
  - **Elément neutre** : il existe $e \in G$ tel que pour tout $x \in G$, on a $x \circ e = x = e \circ x$
  - **Inverse** : pour tout $x \in G$, il existe y tel que $x \circ y = e = y \circ x$
  - **Associativité** : pour tous $x, y, z \in G$, on a $(x \circ y) \circ z = x \circ (y \circ z)$
- Quand $\circ$ est implicite, on dit que G est un groupe

Groupe (2)

- Groupe est *abélien* ou *commutatif* si pour tout x, y, on a $x \circ y = y \circ x$
- L'*ordre* de G est sa taille $|G|$
- G est *fini* si $|G|$ est fini
- Pour tout $g \in G$ on écrit $g^i := g \circ g \circ g \ldots \circ g$ (g composé i fois avec lui-même)
- Un groupe est *cyclique* si il existe $g \in G$ tel que $G = \{g, g^2, g^3, \ldots, g^{|G|}\}$
- Un tel g est appelé un *générateur* de G

Rang d'un groupe

- Le rang d'un groupe $(G, +)$ est le nombre minimal d'éléments nécessaires pour générer le groupe

$$\min\{k : \exists S = \{g_1, \ldots, g_k\} \subset G \text{ t.q. } \forall g \in G, g = \sum_i g_{e_i} \text{ avec } g_{e_i} \in S\}$$

- Exemples
  - $(\mathbb{Z} \times \mathbb{Z}, +)$ est un groupe de rang 2 avec comme générateurs $\{(1, 0), (0, 1)\}$
  - Un groupe cyclique est un groupe fini de rang 1

Exemples de groupes

- $(\mathbb{Z}, +)$ est un groupe, élément neutre est 0
- $(\mathbb{Q}, +)$ est un groupe, élément neutre est 0
- $(\mathbb{Q}, *)$ n'est pas un groupe : 0 n'est pas inversible
- $(\mathbb{Q}^*, *)$ est un groupe, élément neutre est 1
  (ici $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$)
- $(\mathbb{Z}_n, +)$ est un groupe pour tout entier positif n
  (ici $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ sont les entiers modulo n)
- $(\mathbb{Z}_p^*, *)$ est un groupe pour tout nombre premier p
  (ici $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$)
- $(\mathbb{Z}_n \setminus \{0\}, *)$ n'est pas un groupe si n n'est pas premier
- ...

Théorème de Lagrange

- Soit $(G, \circ)$ groupe fini
- Pour tout entier k et tout $g \in G$, on écrit g^k pour $g \circ g \circ \ldots \circ g$, k times
- Théorème de Lagrange : pour tout $g \in G$, on a $g^{|G|} = e$ où e est l'élément neutre du groupe
- Petit théorème de Fermat : pour tout premier p et tout $g \neq 0 \bmod p$, on a $g^{p-1} = 1 \bmod p$

Corps

- Un corps $(K, +, *)$ est un ensemble K muni de deux opérations $+ : K \times K \rightarrow K$ et $* : K \times K \rightarrow K$ telles que
  - $(K, +)$ est un groupe abélien
  - $(K \setminus \{e\}, *)$ est un groupe, où e est l'élément neutre pour $+$
- Un corps $(K, +, *)$ est fini si $|K|$ est fini

Exemples de corps

- $(\mathbb{C}, +, *)$ est un corps avec éléments neutres 0 and 1 pour $+$ et *
- $(\mathbb{Q}, +, *)$ est un corps avec éléments neutres 0 and 1 pour $+$ et *
- $(\mathbb{Z}_p, +, *)$ est un corps fini pour tout premier p
  Ce corps est souvent dénoté $\mathbb{F}_p$
- Pour toute puissance de premier p^n,
  il existe un corps fini $\mathbb{F}_{p^n}$ de taille p^n

Corps finis non premiers

- Soit f un polynôme de degré n avec coefficients dans $\mathbb{F}_p$, f *irréductible* (pas de facteur de degré différent de 0 ou n)
- Soit $(K, +, *)$ où
  - $K = \{\text{polynômes sur } \mathbb{F}_p \text{ de degrés inférieurs à } n\}$
  - $+$ et $*$ sont addition et multiplication modulo f
- Alors $(K, +, *)$ est un corps fini avec p^n éléments
- Exemple : $f(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$ irréductible et $\mathbb{F}_4 = \mathbb{F}_2[x]/(f(x)\mathbb{F}_2[x])$ est un corps fini avec quatre éléments $\{0, 1, x, x + 1\}$
- La *caractéristique* de $\mathbb{F}_{p^n}$ est p

Espace vectoriel

- Un espace vectoriel $(V, +, *)$ sur un corps K est un ensemble $V \supset K$ muni de deux opérations $+ : V \times V \to V$ et $* : K \times V \to V$ telles que
  - $(V, +)$ est un groupe
  - Pour tout $a, b \in K$ et tout $v \in V$, on a $(a + b) * v = a * v + b * v$
  - Pour tout $a \in K$ et $v, w \in V$, on ae $a * (v + w) = a * v + a * w$
- La dimension de l'espace vectoriel est le rang de $(V, +)$
- Une base de V est un ensemble de dim V éléments qui génèrent V

Anneau

- Un anneau $(R, +, *)$ est un ensemble R muni de deux opérations $+ : R \times R \rightarrow R$ et $* : R \times R \rightarrow R$ telles que
  - $(R, +)$ est un groupe abélien
  - $(R, *)$ est associative et a un élément neutre (mais les éléments ne sont pas forcément inversibles)
  - Distributivité : pour tout $a, b, c \in R$, on a $(a + b) * c = a * c + b * c$

Exemples d'anneaux

- Soit K un corps et soit $K[X]$ l'ensemble des polynômes avec coefficients dans K. Alors $(K[X], +, *)$ est un anneau
- $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$ (entiers modulo n) est un anneau pour tout $n \in \mathbb{N}$. C'est un corps si et seulement si n est premier.
- Soir K un corps. Soit $f \in K[X]$ et soit $\tilde{K} = K[X]/(f(X))$ l'ensemble des polynômes sur K "modulo $f(x)$".
  Alors $\tilde{K}$ est un anneau. C'est un corps si et seulement si f est irréductible.

Matrices et systèmes linéaires

- Soit un système de m équations linéaires à n inconnues sur un corps K

$$\sum_{i=1,\ldots,n} a_{ij} x_j = b_i, \qquad i = 1, \ldots, m$$

- On peut le représenter sous forme matricielle

$$Ax = b$$

avec $A \in K^{m \times n}$ et $b \in K^n$

Noyau et image

- Soit le système

$$Ax = b$$

- Noyau de A est Ker $A = \{x \mid Ax = 0\}$
- Image de A est Im $A = \{Ax\}$
- Ker et Im sont des espaces vectoriels et

$$\dim \text{Ker } A + \dim \text{Im } A = n$$

- Si x_0 est une solution du système, alors l'ensemble des solutions est $x_0 + \text{Ker } A$

Elimination gaussienne

- Observation : si $My = x$ alors pour toute matrice inversible N, on a $NMy = Nx$
- En particulier, c'est vrai si N est une matrice qui
  - Echange deux lignes de M
  - Multiplie une ligne par une constante inversible
  - Ajoute un multiple scalaire d'une ligne à une autre ligne
- L'élimination gaussienne répète ces opérations jusqu'à obtenir une matrice triangulaire supérieure

Questions ?

?

Crédits et remerciements

- Mes transparents suivent fortement les notes de cours développées par le Professeur Yves Roggeman pour le cours INFO-F303 à l'Université libre de Bruxelles
- Une partie des transparents et des exercices ont été repris ou adaptés des transparents développés par le Professeur Jean Cardinal pour ce même cours
- Je remercie chaleureusement Yves et Jean pour la mise à disposition de ce matériel pédagogique, et de manière plus large pour toute l'aide apportée pour la reprise de ce cours
- Les typos et erreurs sont exclusivement miennes (merci de les signaler !)