Cours MODEL [1]

Léo Andéol

29 décembre 2018

1. Professeur x, y

Chapitre 1

Bases ?

1.1 Groupes

Définition Soit G un ensemble et $\otimes : G * G \to G$ On dit que $(G, \otimes)$ est un groupe si :

1. L'opérateur $\otimes$ est associatif $\forall (x, y, z) \in G * G * G$,
   $(x \otimes y) \otimes z = x \otimes (y \otimes z)$
2. $\forall x \in G, \exists e \in G$ tel que $e \otimes x = x \otimes e = x$,
   On appelle cet élément e élément neutre du groupe $(G, \otimes)$
3. $\forall x \in G, \exists y \in G$ tel que $x \otimes y = e$
   On dira que y est l'inverse de x (on le note parfois x^-1)

On dira que G est commutatif (ou abélien) si
$\forall (x, y) \in G * G, x \otimes y = y \otimes x$

Exemples

— $(\mathbb{Z}, +)$ est un groupe commutatif,
son élément neutre est 0,
$\forall x \in \mathbb{Z}$ l'inverse de x est $-x$

— $(\mathbb{Z}, *)$ n'est pas un groupe (car 2 n'a pas d'inverse pour x dans $\mathbb{Z}$)

— $(\mathbb{Q} - \{0\}, *)$ est un groupe,
1 est l'élément neutre,
$\forall x \in \mathbb{Q} - \{0\}, \frac{1}{x}$ est l'inverse de x

— On considère l'ensemble des bijections $\sum_n$ de $\{1 \dots n\}$ sur $\{1 \dots n\}$
Comme opérateur binaire on choisit la loi de composition $\circ$
Par exemple pour $n = 2$ on a :

$$\phi_0 : \begin{bmatrix} 1 \to 1 \\ 2 \to 2 \end{bmatrix}$$

$$\phi_1 : \begin{bmatrix} 1 \to 2 \\ 2 \to 2 \end{bmatrix}$$

$\phi_1 \circ \phi_0 = \phi_0 \circ \phi_1 = \phi_1$
Donc $(\sum_2, \circ)$ est un groupe

Un groupe $(G, \otimes)$ tel que G est de cardinalité finie est appelé groupe fini.
Pour $p \in \mathbb{N} - \{0\}$,
On note $\frac{\mathbb{Z}}{p\mathbb{Z}} = \{0, 1, 2, \ldots, p-1\}$ Soit $x \in \mathbb{Z}$ et (q, r) les quotients et le reste de x par p $(0 \leq r < p)$.
$\frac{\mathbb{Z}}{p\mathbb{Z}}$ contient tous les restes possibles.
Pour x et y dans $\frac{\mathbb{Z}}{p\mathbb{Z}} - \{0\}$
On note $x \otimes y = x * y \mod p$
$\Longrightarrow$ on prend le reste de la division euclidienne de $x * y$ par p
$\otimes : (\frac{\mathbb{Z}}{p\mathbb{Z}} - \{0\} * \frac{\mathbb{Z}}{p\mathbb{Z}} - \{0\}) \to \frac{\mathbb{Z}}{p\mathbb{Z}} - \{0\}$
Quand p est un nombre premier $\frac{\mathbb{Z}}{3\mathbb{Z}} - \{0\} = \{1, 2\}$
$1 \otimes 2 = 1 * 2 \mod 3 = 2 \in \frac{\mathbb{Z}}{3\mathbb{Z}} - \{0\}$
$2 \otimes 2 = 4 \mod 3 = 1 \in \frac{\mathbb{Z}}{3\mathbb{Z}} - \{0\}$
$\Longrightarrow$ On en déduit que $(\frac{\mathbb{Z}}{3\mathbb{Z}} - \{0\}, \otimes)$ est un groupe fini/

Soit $(G, \otimes)$ un groupe fini et $H < G$
On dit que H est stable par $\otimes$ ssi :
$\forall (x, y) \in H * H, x \otimes y \in H$
$\Longrightarrow$ On peut considérer que la restriction de $\otimes$ à H est un opérateur binaire sur H.

Définition On dit que $(H, \otimes)$ est un sous groupe de $(G, \otimes)$ si

1. H est stable par $\otimes$
2. $(H, \otimes)$ est un groupe

Soit $(G, \otimes)$ un groupe fini

1.2 Anneaux

1.3 Corps

1.4 Espaces Vectoriels

Chapitre 2

Arithmétiques et modèles de complexité

Enjeu Multiplier 2 par 3 en machine n'a pas le même coût que multiplier deux nombres qui ont 30 millions de chiffres.

Complexité On veut évaluer les complexités en temps (pas en mémoire)
On s'appuie sur le modèle RAM (random access machine) : un programme écrit dans ce modèle :

1. écrire ou lire sur des bandes / zones mémoires (on suppose) instantanément
2. l'addition, la soustraction, la multiplication et la division sur des mots machines s'effectuent en une unité temporelle
3. les sauts de mémoire se font instantanément

On peut définir deux types de complexité en temps.

Complexité arithmétique On compte les opérations binaires effectuées par un algorithme

Exemple Soit $(G, \otimes)$ un groupe
On compte le nombre de fois que l'on applique $\otimes$
$\implies$ Ce modèle est considéré pertinent si toutes les données numériques ont une taille inférieure ou égale au mot machine (64 bits sur les machines actuelles en 2018)

- $\frac{\mathbb{Z}}{p\mathbb{Z}}$ avec p premier est un corps
  Si $p \leq 2^{64}$ (par exemple $p = 65521 \leq 2^{16}$)le modèle de complexité arithmétique est "presque pertinent".
- a, b dans $\frac{\mathbb{Z}}{p\mathbb{Z}}$
  $a + b \leq 2^{17}$
  $a * b \leq 2^{32}$
  $\implies$ Si pertinent mais pas dans $\frac{\mathbb{Z}}{p\mathbb{Z}}$
  mais dans $\frac{\mathbb{Z}}{p\mathbb{Z}}$ on a
  $a + b \mod p$ et $a * b \mod p \implies$ 2 opérations sur les mots machines

pour un + ou $*$ donc pour cela que pas totalement pertinent, d'où la notation O pour enlever les facteurs proportionnels

— $(\mathbb{Q}, +, *)$
$\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1 b_2 + a_2 b_1}{b_1 b_2} \implies$ 3 multiplications + 1 addition
$\frac{a_1}{b_1} * \frac{a_2}{b_2} = \frac{a_1 a_1}{b_1 b_2} \implies$ 2 multiplication
Donc + coute deux fois plus que $*$
De plus comme $\mathbb{Q}$ est infini, a et b peuvent dépasser 2^{64} et donc être supérieur à un mot machine.

Complexité binaire

Objectif Tenir compte de la taille des données manipulées
On le dénit sur $\mathbb{Z}$
On se donne $b \in \mathbb{N} - \{0\}$

Lemme $\forall n \in \mathbb{N}$ il existe une unique $(b_0 \cdots_k)$ telle que :

1. $n = b_0 + b_1 b + b_2 b^2 + \cdots + b_k b^k$
2. $b_i \in \{0 \dots b-1\}$ avec $b_k \neq 0$

Il s'agit de la représentation en base b d'un entier naturel.
Si $n \in \mathbb{Z}, n \geq 0 \implies$ on a sa représentation en base b.
Si $n < 0, -n \geq 0 \implies$ on a sa représentation.
Pour $\mathbb{Q}$ il suffit de remarquer que $\mathbb{Q} = \{(a,b), a \in \mathbb{Z}, b \in \mathbb{Z} - \{0\}, pgcd(a,b) = 1\} \approx (\mathbb{Z} * \mathbb{Z} - \{0\})$
Le modèle de complexité binaire consiste à compter les opérations dans $\frac{\mathbb{Z}}{b\mathbb{Z}}$

Exemple $7 * 9$ en base 2.
$9 = 1 + 0 * 2 + 0 * 2^2 + 1 * 2^3 \implies (1,0,0,1)$
$7 = 1 + 1 * 2 + 1 * 2^2 \implies (1,1,1)$
Bit de poids fort à la fin
$9 * 7 = 1 * 2^3(1 + 2 + 2^2) + 0x2^3(1 + 2 + 2^2) + 0 * 2(1 + 2 + 2^2) + 1(1 + 2 + 2^2)$
$3 * 4 = 12$ multiplications et 3 additions, donc 15 opérations