Master Cryptographie & Sécurité

Élément de combinatoire

djebailikarima.cs@gmail.com / k.djebaili@univ-batna2.dz

Présenté par Dr K.DJEBAILI

Élément de combinatoire

- **Introduction**
- **Partie I : Combinatoire énumérative.**
  - Application d'un ensemble *E* dans un ensemble *F*.
  - Applications particulières (injectives, surjectives, bijectives).
  - Relations binaires.
  - Notion de cardinal. Ensembles finis. Ensembles dénombrables.
  - Propriétés de dénombrement des ensembles finis.
- **Partie II :Théorie des graphes.**
  - Graphes simples.
  - Matrice associée au graphe.
  - Arbre.
  - Coloration d'un graphe.
  - Graphes particuliers (graphes hamiltoniens, graphes orientés,…).
  -

Partie III :Théorie des graphes pour la cryptographie.

- Problèmes complexes liés aux graphes.
- Graphes et cryptographie.

Introduction

Les fondements mathématiques de la modélisation et le traitement de l'information numérique font intervenir plusieurs branches des mathématiques comme l'Algèbre, la Combinatoire et la Théorie des graphes. Ce support du cours développe les constructions de base de ces branches ainsi certains outils de la théorie des graphes pour la cryptographie.

Partie I : Combinatoire énumérative

Plan

1. Application d'un ensemble *E* dans un ensemble *F*
2. Applications particulières (injectives, surjectives, bijectives).
3. Relations binaires
4. Notion de cardinal. Ensembles finis. Ensembles dénombrables.
5. Dénombrement des ensembles.

1. Application d'un ensemble E dans un ensemble F

Défnition 1.1 : Soit E et F des ensembles non vides, une application f de E dans F est la donnée, pour tout élément x de E d'un unique élément y, noté $f(x)$ de F. On dit alors que y est l'image de x par f et que x est un antécédant de y.

Notation:

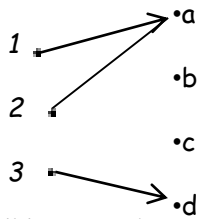
$$f : E \longrightarrow F$$
$$x \longrightarrow f(x)$$

Interprétation au moyen d'un graphe orienté:

On représente les éléments de E et de F par des points et on relie un élément x de E à un élément y de F par une flèche de x vers y, si $y = f(x)$.

Exemple :

$E = \{1,2,3\}$, $F = \{a,b,c,d\}$, f définie par : $f(1) = f(2) = a$, $f(3) = d$.



Remarque : Un élément x de E a une unique image par f. Mais un élément y de F peut avoir un ou plusieurs antécédants, ou ne pas en avoir.

Définitions 1.2 :Soit A une partie de E, l'image de A par f est le sous ensemble de F : $f(A) = \{y \in F \mid \exists x \in A : f(x) = y\}$.

L'ensemble $f(E)$ est noté im f.

Soit B une partie de F . L'image réciproque de B par f est le sous ensemble de E :

$$f^{-1}(B) = \{x \in E \mid f(x) \in B\}.$$

2. Applications particulières (injectives, surjectives, bijectives).

Définitions 1.3 :

a)On dit qu'une application f de E dans F est injective (ou est une injection) si :

$$\forall x \in E, \forall x' \in E, f(x) = f(x') \Rightarrow x = x'.$$

Ceci équivaut à

$$\forall x \in E, \forall x' \in E, x \neq x' \Rightarrow f(x) \neq f(x').$$

Interprétation au moyen d'un graphe orienté :

Tout élément de F est extrémité finale d'au plus une flèche.

b)On dit qu'une application f de E dans F est surjective (ou est une surjection) si:

$$\forall y \in F, \exists x \in E : y = f(x).$$

Ceci équivaut à

$$im\ f = F.$$

Interprétation au moyen d'un graphe orienté.

Tout élément de F est extrémité finale d'au moins une flèche.

c)On dit qu'une application f de E dans F est bijective (ou est une bijection) si elle est à la fois injective et surjective. Ceci équivaut à :

$$\forall y \in F, \exists! x \in E : y = f(x).$$

Interprétation au moyen d'un graphe orienté :

Tout élément de F est extrémité finale d'exactement une flèche.

Dans ce cas, on peut définir une application de F dans E, appelée application réciproque de f et notée f^{-1}. L'application f^{-1} est caractérisée par :

$$x = f^{-1}(y) \Longleftrightarrow y = f(x).$$

Remarque : Ne pas confondre l'image réciproque d'une partie de F, qui est définie pour toute application f de E dans F et l'application réciproque de l'application f qui n'est définie que si f est bijective.

Théorème 2.1 : (Principe de recollement) Soit deux applications :

$$f : E \longrightarrow F$$

$$g : E' \longrightarrow F'$$

où E et E' sont deux ensembles non vides, disjoints, et F et F' sont deux ensembles non vides, disjoints. On définit l'aplication :

$$h : E \cup E' \longrightarrow F \cup F'$$

par :

$$\text{si } x \in E,\ h(x) = f(x),$$

$$\text{si } x \in E',\ h(x) = g(x).$$

1) L'application h est injective, si et seulement si f et g sont injectives.
2) L'application h est surjective, si et seulement si f et g sont surjectives.
3) L'application h est bijective, si et seulement si f et g sont bijectives.

La preuve est laissée au TD.

3. Relations binaires

Définition 3.1 : Une relation binaire R sur un ensemble non vide, E, est un sous ensemble de $E \times E$.

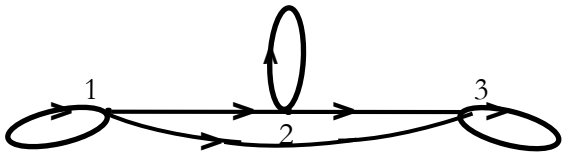
Notation : $(x,y) \in R$ est notée xRy.

Interprétation au moyen d'un graphe orienté :
On représente les éléments de E par des points et on relie un élément x de E à un élément y de E par une flèche de x vers y, si xRy.

Exemple : La relation $\leq$ sur l'ensemble d'entiers {1,2,3} est le sous ensemble de {1,2,3} × {1,2,3} :

$$\{(1,1),(1,2),(1,3),(2,2),(2,3),(3,3)\},$$

représenté par le graphe :



Défnitions 3.2 : Une relation binaire sur E est dite :
réflexive si : $\forall x \in E,\ xRx$,
symétrique si : $\forall (x,y) \in E \times E,\ xRy \Rightarrow yRx$,
antisymétrique si : $\forall (x,y) \in E \times E,\ (xRy) \text{ et } (yRx) \Rightarrow x = y$,
transitive si : $\forall (x,y,z) \in E \times E \times E,\ (xRy) \text{ et } (yRz) \Rightarrow xRz$.

Définitions 3.3 : On appelle *relation d'équivalence*, une relation binaire, réflexive, symétrique et transitive.

Soit R une relation d'équivalence sur E. Pour tout x de E, on appelle *classe d'équivalence de x*, l'ensemble

$$\bar{x} = \{x \in E \ / x R y\}.$$

Propriété 3.4 :

1) L'ensemble des classes d'équivalence est alors une partition de E.
2) Réciproquement, toute partition de E détermine une relation d'équivalence.

Définitions 3.5 :

a) On appelle *relation d'ordre*, une relation binaire, réflexive, antisymétrique et transitive. *Un ensemble ordonné* est un ensemble muni d'une relation d'ordre

b) Soit E un ensemble ordonné. Notons $\leq$ la relation d'ordre. Soit A une partie non vide de E, un majorant de A est un élément m de E, tel que :

$$\forall x \in A, x \leq m,$$

un minorant de A est un élément m' de E, tel que :

$$\forall x \in A, m' \leq x.$$

c) Un sous ensemble A de E admettant un majorant est dit majoré et un sous ensemble A de E admettant un minorant est dit minoré.

d) On dit que m est plus grand élément de A, si m est un majorant de A appartenant à A. Cet élément, s'il existe, est unique.
On dit que m' est plus petit élément de A, si m' est un minorant de A appartenant à A. Cet élément, s'il existe, est unique.

Propriétés 3.6 : (Propriétés des entiers liées à la relation d'ordre)

1) Tout sous ensemble non vide, majoré de Z admet un plus grand élément.
2) Tout sous ensemble non vide, minoré de Z admet un plus petit élément.
3) En particulier, tout sous ensemble non vide de N admet un plus petit élément.

4. Notion de cardinal. Ensembles finis. Ensembles dénombrables.

Définition 4.1 : On dit qu'un ensemble E est fini si:

- soit E est vide
- soit il existe un entier strictement positif n et une bijection

$$\phi : [1,n] \longrightarrow E$$
$$i \longrightarrow a_i$$

Un ensemble non fini est dit infini.

Théorème 4.2 : Soit n et p des entiers strictement positifs.

(i) Il existe une injection de [1,n] dans [1,p] , si et seulement si $n \leq p$.
(ii) Il existe une surjection de [1,n] dans [1,p] , si et seulement si $p \leq n$.
(iii) Il existe une bijection de [1,n] dans [1,p] , si et seulement si $n = p$.

Corollaire 1 : Soit E un ensemble fini non vide. L'entier n, strictement positif, tel qu'il existe une bijection de [1,n] dans E, est unique

Définition 4.3 : Avec les hypothèses du corollaire 1, on dit que E *est de cardinal n et que n est le nombre d'éléments de* E et on note $E = \{a_1, \ldots, a_n\}$. Dans le cas où E est vide, on convient que E est de cardinal zéro.

Notation : Le cardinal d'un ensemble fini E est noté Card E ou $|E|$.

Corollaire 2 : Soit E et F des ensembles finis, non vides.

Il existe une injection de E dans F, si et seulement si $|E| \leq |F|$.

Il existe une surjection de E dans F, si et seulement si $|F| \leq |E|$.

Il existe une bijection de E dans F, si et seulement si $|E| = |F|$.

Définition 4.4 : On dit que deux ensembles E et F, finis ou non, ont même cardinal, s'il existe une bijection de E dans F.

Remarque : Les définitions 4.1 et 4.4 sont cohérentes : Les ensembles E et F finis, non vides, sont de même cardinal, si et seulement s'il existe une bijection de E dans F.

Corollaire 3 : Soit E un ensemble fini de cardinal $n \geq 1$ et soit a un élément de E. L'ensemble $E \setminus \{a\}$ est fini, de cardinal $n - 1$.

Corollaire 4 : Soit E et F des ensembles finis, non vides, de même cardinal et soit f une application de E dans F. Les propositions suivantes sont équivalentes :

(i) L'application f est injective.

(ii) L'application f est surjective.

(iii) L'application f est bijective.

Corollaire 5 : L'ensemble N est infini.

Corollaire 6 : Soit E et F des ensembles finis, non vides, s'il existe une application injective f de E dans F, et une application injective g

de F dans E, il existe une application bijective de E dans F

Corollaire 7 : (Principe des tiroirs) Soit E et F des ensembles finis, non vides, et *soit* $f : E \longrightarrow F$, si $|E| > |F|$, il existe deux éléments distincts x et x' de E, tels que $f(x) = f(x')$.

Définition 4.5 : On dit qu'un ensemble E est dénombrable, s'il a même cardinal que N.

Exemples:

a) L'ensemble Z est dénombrable.

b) Les ensembles N^2 et Q sont dénombrables.

c) L'ensemble R n'est pas dénombrable

5. Propriétés de dénombrement des ensembles finis

Dénombrement des ensemble c'est à dire calculer le nombre d'éléments de certains ensembles finis.

Exemples :

Nombre de parties à p éléments d'un ensemble à n éléments.

Nombre d'applications d'un ensemble à n éléments dans un ensemble à p éléments.

Théorème 6.1 : (Principe d'inclusion)

1) Soit E un ensemble fini et soit F une partie de E. L'ensemble F est fini et on a : $|F| \leq |E|$.
2) De plus, dans ce cas, on a : $|E| = |F| \iff E = F$

La preuve est laissée au TD.

Théorème 6.2 : (Principe d'addition) Soit A et B deux parties finies, *disjointes*, d'un ensemble E. L'ensemble $A \cup B$ est fini et on a : $|A \cup B| = |A| + |B|$.

La preuve est laissée au TD.

Théorème 6.4 : (Principe de multiplication) Soit E et F des ensembles finis, non vides, $E \times F$ est fini et on a : $|E \times F| = |E|\,|F|$.

La preuve est laissée au TD.