U.E. Mathématiques Discrètes

A. Bucciarelli, B. Delcroix-Oger , S. Laplante et C. Tasson

Université Paris Diderot

Semestre d'automne 2019

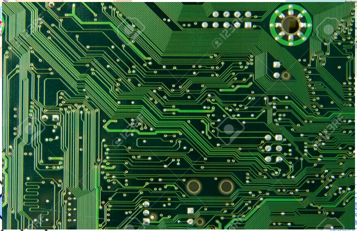
Plan de route

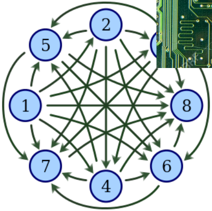
Organisation de l'UE

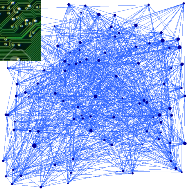
- 10 séances de Cours-TD de 3 heures chacunes
- Évaluation en trois parties :
  - 4 QCM d'une quinzaine de minutes (premier en séance 3)
  - Projet d'application des Maths discrètes à l'informatique (rédaction d'un billet de blog)
  - Examen final
- Calcul de la note finale :

$$\frac{3}{20}\left(\frac{QCM_1 + QCM_2 + QCM_3 + QCM_4}{4} + projet\right) + \frac{7}{10}examen$$

Pourquoi des graphes ?







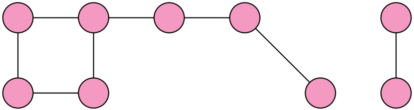
©Can Stock Photo, RATP, SNCF, Booyabazooka pour wikipedia, Yoann Morel

Graphes

Définition

Un graphe non orienté est une paire (V, E) où

- V est un ensemble dont les éléments sont appelés sommets
- E est un ensemble de paires de sommets distincts, appelées arêtes.

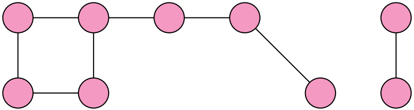


Graphes

Définition

Un graphe non orienté est une paire (V, E) où

- V est un ensemble dont les éléments sont appelés sommets
- E est un ensemble de paires de sommets distincts, appelées arêtes.



Qu'est-ce qu'un ensemble ?

Définition

Un ensemble est une collection (= regroupement) *non ordonnée* d'objets (sans répétition). Un objet de l'ensemble est appelé un élément de l'ensemble, on dit alors qu'il lui appartient. Un multiensemble est une collection d'objets avec répétitions éventuelles.

Si un objet x appartient à un ensemble E, on note $\boldsymbol{x \in E}$.
Sinon, on note $\boldsymbol{x \notin E}$.
Un ensemble sera noté entre accolades $\{\ \}$.$\{1, \ldots, n\} = [\![1, n]\!]$

Qu'est-ce qu'un ensemble ?

Définition

Un ensemble est une collection (= regroupement) *non ordonnée* d'objets (sans répétition). Un objet de l'ensemble est appelé un élément de l'ensemble, on dit alors qu'il lui appartient. Un multiensemble est une collection d'objets avec répétitions éventuelles.

Si un objet x appartient à un ensemble E, on note $\boldsymbol{x \in E}$.
Sinon, on note $\boldsymbol{x \notin E}$.
Un ensemble sera noté entre accolades $\{\ \}$.$\{1, \ldots, n\} = [\![1, n]\!]$

Exemple

Sauriez-vous donner des exemples et des contre-exemples d'ensemble ?

Qu'est-ce qu'un ensemble ?

Définition

Un ensemble est une collection (= regroupement) *non ordonnée* d'objets (sans répétition). Un objet de l'ensemble est appelé un élément de l'ensemble, on dit alors qu'il lui appartient. Un multiensemble est une collection d'objets avec répétitions éventuelles.

Si un objet x appartient à un ensemble E, on note $\boldsymbol{x \in E}$.
Sinon, on note $\boldsymbol{x \notin E}$.
Un ensemble sera noté entre accolades $\{\ \}$.$\{1, \ldots, n\} = [\![1, n]\!]$

Exemple

Sauriez-vous donner des exemples et des contre-exemples d'ensemble ?

Attention

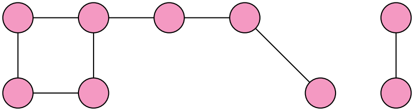
Nous ne considérerons ici que des ensembles finis.

Graphes

Définition

Un graphe non orienté est une paire (V, E) où

- V est un ensemble dont les éléments sont appelés sommets
- E est un ensemble de paires de sommets distincts, appelées arêtes.

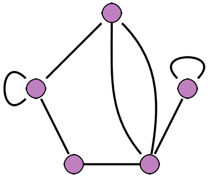


Graphes

Définition

Un multigraphe est une paire (V, E) où

- V est un ensemble dont les éléments sont appelés sommets
- E est un multiensemble de paires de sommets distincts ou un singleton, appelées arêtes.

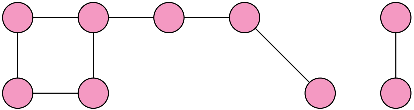


Graphes

Définition

Un graphe non orienté est une paire (V, E) où

- V est un ensemble dont les éléments sont appelés sommets
- E est un ensemble de paires de sommets distincts, appelées arêtes.

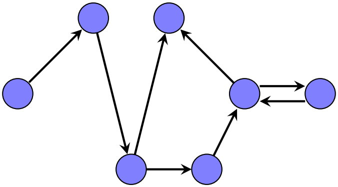


Graphes

Définition

Un graphe orienté est une paire (V, E) où

- V est un ensemble dont les éléments sont appelés sommets
- E est un ensemble de couples de sommets distincts, appelées arêtes.

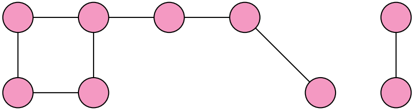


Graphes

Définition

Un graphe non orienté est une paire (V, E) où

- V est un ensemble dont les éléments sont appelés sommets
- E est un ensemble de paires de sommets distincts, appelées arêtes.



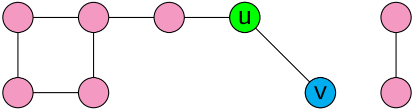
Graphes

Définition

Un graphe non orienté est une paire (V, E) où

- V est un ensemble dont les éléments sont appelés sommets
- E est un ensemble de paires de sommets distincts, appelées arêtes.

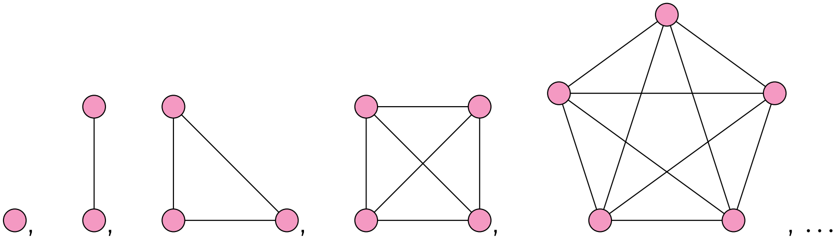
Soit G un graphe. Si $\{u, v\}$ est une arête de G, alors les sommets u et v sont dits adjacents. On dit aussi que u est un voisin de v (ou que v est un voisin de u).



Un premier exemple de graphes : Graphe complet

Définition

Un graphe est complet si toute paire de sommets distincts est une arête.



Un peu de pratique

Exercice(s)

Exercice 1 de la feuille de TD 1

Opérations sur les ensembles

Considérons les ensembles $A = \{x_1, \ldots, x_n\}(= \{x_3, x_n, x_1, x_2, x_4, \ldots, x_{n-1}\})$ et $B = \{y_1, \ldots, y_k\}$:

Définition

$\cup$ (Union) : $A \cup B =$	$\{z \mid (\exists 1 \leq j \leq k : z = y_j)$ or $(\exists 1 \leq i \leq n : z = x_i)\}$
$\cap$ (Intersection) :	$A \cap B = \{z \mid \exists 1 \leq i \leq n, 1 \leq j \leq k : z = y_j = x_i\}$
$\bar{}$ (Complémentaire) :	Dans A, $\bar{S} = \{x \in A \mid x \notin S\}(= A \setminus S)$
$\subseteq$ (Sous-ensemble) :	$S \subseteq A$ ssi $\{\exists T : T \cap S = \emptyset, S \cup T = A\}$
$\times$ (Produit cartésien) :	$A \times B = \{(x, y) \mid x \in A$ et $y \in B\}$

Opérations sur les ensembles

Considérons les ensembles $A = \{x_1, \dots, x_n\} (= \{x_3, x_n, x_1, \dots, x_2\})$ et $B = \{y_1, \dots, y_k\}$:

Définition

$\cup$ (Union) : $A \cup B = \{z | (\exists 1 \leq j \leq k : z = y_j) \text{ or } (\exists 1 \leq i \leq n : z = x_i)\}$

$\cap$ (Intersection) : $A \cap B = \{z | \exists 1 \leq i \leq n, 1 \leq j \leq k : z = y_j = x_i\}$

$\bar{}$ (Complémentaire) : Dans A, $\bar{S} = \{x \in A | x \notin S\} (= A \setminus S = T)$

$\subseteq$ (Sous-ensemble) : $S \subseteq A$ ssi $\{\exists T : S \cup T = A, S \cap T = \emptyset\}$

Question

Quels sont les analogues des opérations ci-dessus en calcul propositionnel ?

Définition

$\times$ (Produit cartésien) : $A \times B = \{(x, y) | x \in A \text{ et } y \in B\}$

Opérations sur les ensembles

Question

Comment illustrer ces notions sur les graphes

Considérons les ensembles $A = \{x_1, \ldots, x_n\} (= \{x_3, x_n, x_1, \ldots, x_2\})$ et $B = \{y_1, \ldots, y_k\}$:

Définition

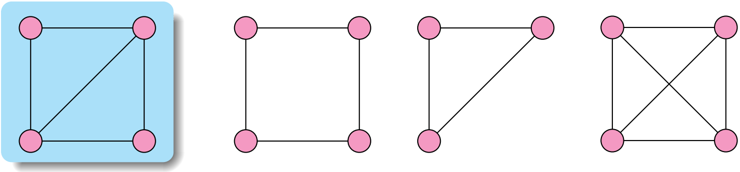
$\cup$ (Union) :	union de graphes
$\cap$ (Intersection) :	restriction de graphes
$\bar{\ }$ (Complémentaire) :	Dans A, $\bar{S} = \{x \in A \mid x \notin S\} (= A \setminus S = T)$
$\subseteq$ (Sous-ensemble) :	sous-graphes
$\times$ (Produit cartésien) :	produits de graphes

Sous-graphes

Soient $G = (V, E)$ et $G' = (V', E')$ deux graphes.

Définition

On dit que G est un sous-graphe de G' si $V \subseteq V'$ et $E \subseteq E'$. On dit que G est un sous-graphe induit de G' si de plus toute arête e de E' entre deux sommets de V est dans E.

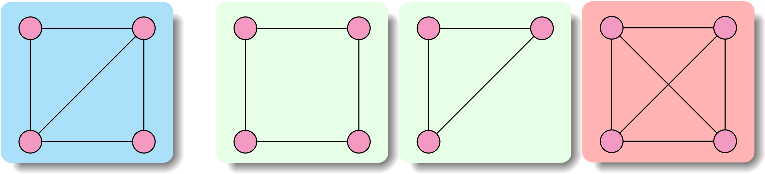


Sous-graphes

Soient $G = (V, E)$ et $G' = (V', E')$ deux graphes.

Définition

On dit que G est un sous-graphe de G' si $V \subseteq V'$ et $E \subseteq E'$. On dit que G est un sous-graphe induit de G' si de plus toute arête e de E' entre deux sommets de V est dans E.



Un peu de pratique

Exercice(s)

Exercice 2 de la feuille de TD 1

Combien d'éléments dans un ensemble ?

Définition

Le cardinal d'un ensemble E est son nombre d'éléments.

Le cardinal d'un ensemble E est noté $|E|$. On a $|\emptyset| = 0$.

Proposition

Soient A et B deux ensembles,

- $|A \cup B| = |A| + |B| - |A \cap B|$
- $|A \cap B| \leq \min(|A|, |B|)$
- $|A \times B| = |A| \times |B|$
- *Si* $S \subseteq A$, $|S| \leq |A|$
- $|\bar{S}| = |A| - |S|$

Applications

Principe de multiplication

Si un objet consiste en k éléments, chacun choisit dans un ensemble A_i de cardinal $|A_i|$ $(1 \leq i \leq k)$, alors le nombre d'objets différents possibles est :

$$|A_1 \times \ldots \times A_k| = |A_1| \times \ldots \times |A_k|.$$

Exemple

Dans une base de données, contenant une table "clients" de taille k et une table "commandes" de taille l, quelle est la taille du produit cartésien des deux tables ?

Exemple

Un graphe a 3 sommets rouges, 6 sommets verts et 4 sommets bleus, ainsi que toutes les arêtes possibles entre deux sommets de couleurs différentes : combien y a-t-il de triangles sur le graphe ?

Applications

Principe d'addition

Si $E_1, \ldots, E_k$ sont deux à deux disjoints ($E_i \cap E_j = \emptyset$, pour tout $i \neq j$), on note $\sqcup$ l'union disjointe de ces éléments et on a :

$$|E_1 \sqcup \ldots \sqcup E_k| = |E_1| + \ldots + |E_k|$$

Exemple

Un graphe a 3 sommets rouges, 6 sommets verts et 4 sommets bleus, ainsi que toutes les arêtes possibles entre deux sommets de couleurs différentes : combien a-t-il d'arêtes ?

À vous !

Exercice(s)

Exercice 3 de la feuille de TD1

Activité introductive

Exercice(s)

Exercice 4 de la feuille de TD1

Uplets

Définition

Un uplet d'éléments de E est une liste d'éléments de E.

Définition

Soient E et F deux ensembles. Une application de E dans F est un uplet de $|E|$ éléments de F. Comme chaque élément de E désigne une et une seule case du uplet, on peut alors noter $f(x)$ l'(unique !) élément du uplet correspondant à x.

Proposition

Le nombre d'applications d'un ensemble E dans un ensemble F est :

$$\mathcal{F}(E,F) = |F|^{|E|}.$$

Bijections

Définition

L'application f est dite :

- injective si $f(x_1) = f(x_2) \implies x_1 = x_2$,
- surjective si pour tout $y \in F$, il existe $x \in E$ tel que $f(x) = y$,
- bijective si elle est injective et surjective (pour tout $y \in F$, il existe un unique $x \in E$ tel que $f(x) = y$).

On parle alors respectivement d'injection, de surjection et de bijection.

Bijections

Proposition

S'il existe une injection $f : A \to B$, alors $|A| \leq |B|$.

Proposition

S'il existe une surjection $f : A \to B$, alors $|A| \geq |B|$.

Proposition

Si deux ensembles sont en bijection, ils ont même cardinal.

C'est ce que l'on fait dès que l'on numérote des objets !

Permutations et factorielles

Définition

Une permutation d'un ensemble E est une application bijective de E dans E.

Proposition

Le nombre de permutations d'un ensemble à n éléments est donné par la factorielle

$$n! = \prod_{i=1}^{n} i = 1 \times 2 \times \ldots \times n \text{ avec } 0! = 1.$$

Exemple

Alice range ses cours de L3 pour pouvoir les relire facilement. Sachant qu'elle a 6 modules différents ce semestre, de combien de manières différentes pourra-t-elle attribuer les intercalaires de son classeur ?

Uplets sans répétitions (=Arrangements)

Définition

Un k-arrangement de E est un k-uplet de E sans répétition. C'est une injection de $[\![1;k]\!] := \{1, 2, \ldots, k-1, k\}$ dans E.

Remarque : Un $|E|$-arrangement est une permutation.

Proposition

Le nombre de k-arrangements (= k-uplets sans répétitions) d'un ensemble E est donné par :

$$(n)_k = \prod_{i=1}^{k} (n - i + 1) = \frac{n!}{(n-k)!}$$

Exemple

Le comité olympique décide, en première sélection, de classer quatre dossiers parmi les vingt dossiers de candidature déposés : combien de classements différents pourrait-il faire ?

Sous-ensembles (=combinaisons)

Remarque

Un *k-sous-ensemble* (ou ss-ensemble de cardinal k) d'un ensemble E devient un k-uplet sans répétition lorsqu'on ordonne ses éléments

Proposition

Soit E un ensemble de cardinal n. Le nombre de sous-ensembles de E de cardinal k est donné par le coefficient binomial :

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{\overbrace{n(n-1)\dots(n-k+1)}^{k \text{ éléments}}}{k!} = \frac{(n)_k}{k!}$$

Exemple

Pour jouer au loto, il faut cocher 5 numéros sur une grille de 49 nombres puis choisir un numéro chance parmi dix : combien de tickets de loto différents est-il possible de remplir ?

Ensemble des parties

Définition

L'ensemble des sous-ensembles d'un ensemble X est appelé ensemble des parties de X, notée $\mathcal{P}(X)$.

Définition

La fonction indicatrice de $S \subset X$, notée $\mathbf{1}_S$ est l'application de X dans $\{0, 1\}$ qui envoie les éléments de S sur 1 et les autres sur 0.

Proposition

$$|\mathcal{P}(X)| = 2^{|X|}$$

Soit $B = \{0, 1\}$ l'ensemble des booléens.

Définition

Une fonction booléenne à n variables (ou fonction binaire, ou fonction logique) est une application

$$\begin{array}{rcl} f : B^n & \to & B \\ (a_1, \ldots, a_n) & \to & f(a_1, ..., a_n) \end{array}$$

On représente f par un tableau qui est dit Table de Vérité de f.

Proposition

- *L'ensemble F_n des fonctions booléennes (de B^n dans B) est en bijection avec $\mathcal{P}(B^n)$ l'ensemble des ensembles d'éléments de B^n.*
- *Le nombre d'éléments de F_n est $2^{(2^n)}$.*

À vous !

Exercice(s)

Exercices 5 et 6 de la feuille de TD1

À vous !

Exercice(s)

Exercices 5 et 6 de la feuille de TD1

A-t-on retrouvé tous les cas de l'exercice 4 ? ? ?

Multi-ensembles (=combinaisons avec répétition)

Proposition

Soit E un ensemble de cardinal n. Le nombre de k-multi-ensembles de E est donné par le coefficient multinomial :

$$\binom{n+k-1}{k}.$$

Exemple

Bob range son armoire dans laquelle il a dix paires de chaussettes toutes identiques et cinq tiroirs : combien de manières différentes a-t-il de ranger ses affaires ?

Tableau récapitulatif

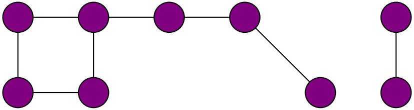
Soit E un ensemble de cardinal n et F un ensemble de cardinal k.

		Ordonné : Oui	Ordonné : Non
Répétition	Oui	k-uplets de E (= fonctions de F dans E) n^k	k-multi-ensembles de E $\binom{n+k-1}{k}$
	Non	k-uplets sans répétitions (= fctions inj. de F dans E) $\frac{n!}{(n-k)!}$	k-sous-ensembles de E $\binom{n}{k}$

Degré

Définition

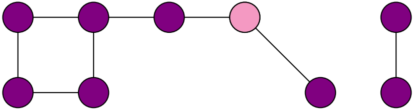
Le **degré** d'un sommet v est le nombre d'arêtes contenant v.



Degré

Définition

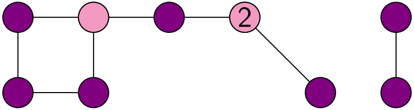
Le *degré* d'un sommet v est le nombre d'arêtes contenant v.



Degré

Définition

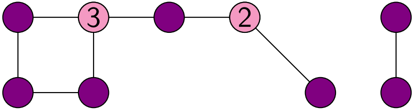
Le degré d'un sommet v est le nombre d'arêtes contenant v.



Degré

Définition

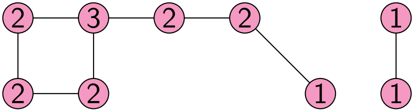
Le degré d'un sommet v est le nombre d'arêtes contenant v.



Degré

Définition

Le degré d'un sommet v est le nombre d'arêtes contenant v.



Degré

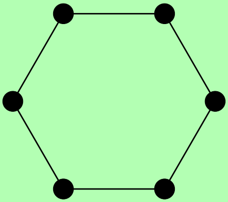
Définition

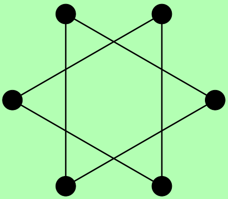
Le degré d'un sommet v est le nombre d'arêtes contenant v.

Attention

Une distribution de degré ne permet pas de caractériser le graphe.

Exemple





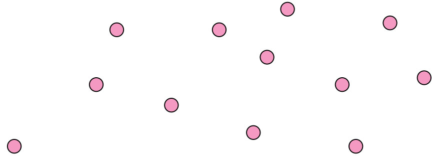
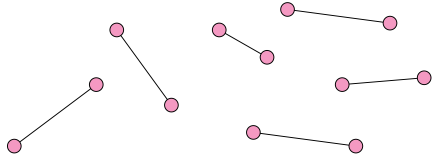
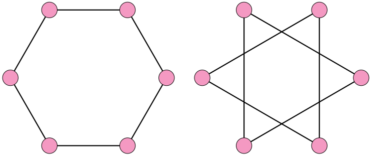
Graphe n-régulier

Définition

Un graphe n-régulier est un graphe dont tous les sommets sont de degré n.

Définition

Un graphe *n-régulier* est un graphe dont tous les sommets sont de degré n.

n=0	
n=1	
n=2	

Degré

Le degré des sommets d'un graphe $G = (V, E)$ vérifie les propriétés suivantes :

Proposition

$$\sum_{v \in V} \deg(v) = 2|E|$$

Corollaire (Lemme des poignées de main)

Tout graphe (non orienté fini) a un nombre pair de sommets de degré impair.

Un peu de pratique

Exercice(s)

Exercices 7 à 9 de la feuille de TD 1

Degré

Le degré des sommets d'un graphe $G = (V, E)$ vérifie les propriétés suivantes :

Proposition

$$\sum_{v \in V} \deg(v) = 2|E|$$

Question

Comment le prouver ?

Principe de double-comptage

Le double-comptage consiste à compter de deux manières différentes un certain ensemble. De manière équivalente, il revient à donner une bijection entre deux ensembles qui ont alors le même cardinal.

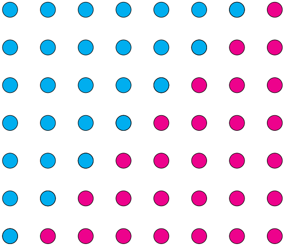
Principe de double-comptage

Le double-comptage consiste à compter de deux manières différentes un certain ensemble. De manière équivalente, il revient à donner une bijection entre deux ensembles qui ont alors le même cardinal.

Exemples

- Preuve du nombre de k-sous-ensembles (équivalence entre k-sous-ensemble ordonné et k-uplet sans répétition).
- Preuve de la formule du binôme de Newton (équivalence entre la donnée d'une fonction de $\{1, \ldots, n\} \to \{0, 1\}$ et la donnée d'un sous-ensemble de $\{1, \ldots, n\}$ correspondant à $\{x \in \{1, \ldots, n\} | f(x) = 1\}$).

Illustration du principe de double-comptage



Comptons les points magenta :

- Il y a en tout 7×8 points (ici, n=7). Comme il y a autant de points magenta que cyan, il y a donc 28 points magenta.
- Comptons les par ligne : il y en a 1 sur la 1ère ligne, 2 sur la 2ème, ..., 7 sur la 7ème soit $1+2+3+4+5+6+7$ points magenta.

On a alors $\frac{7\times 8}{2} = 1+2+3+4+5+6+7$.

Illustration du principe de double-comptage

Proposition

$$\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$$

Démonstration.

Considérons un rectangle de n lignes et $n+1$ colonnes avec i points magenta sur la $i$ème ligne et les autres cyan. Comptons les points magenta :

- Il y a en tout $n \times (n-1)$ points. Comme il y a autant de points magenta que cyan, il y a donc $\frac{n(n-1)}{2}$ points magenta.
- Comptons les par ligne : il y en a 1 sur la 1ère ligne, ..., n sur la $n$ième soit $\sum_{i=1}^{n} i$ points magenta.

En comptant de deux manières différentes les points magenta, on obtient $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$. □

À vous maintenant !

Exercice(s)

Exercice 10 de la feuille de TD 1

Retour vers le futur

Définition

Considérons un sous-ensemble F d'un ensemble **fini** E. La probabilité pour un élément x de E d'être dans F est donnée par :

$$\mathbb{P}(\{x \in F\}) = \frac{|F|}{|E|}$$

Retour vers le futur

Définition

Considérons un sous-ensemble F d'un ensemble **fini** E. La probabilité pour un élément x de E d'être dans F est donnée par :

$$\mathbb{P}(\{x \in F\}) = \frac{|F|}{|E|}$$

Attention

Une probabilité ne peut **JAMAIS** être plus grande que 1.

Retour vers le futur

Définition

Considérons un sous-ensemble F d'un ensemble **fini** E. La probabilité pour un élément x de E d'être dans F est donnée par :

$$\mathbb{P}(\{x \in F\}) = \frac{|F|}{|E|}$$

Attention

Une probabilité ne peut **JAMAIS** être plus grande que 1.

Remarque

Une définition plus rigoureuse sera donnée plus tard dans le cours.

Un peu de pratique

Exercice(s)

Exercice 1 de la feuille de TD 2

Raisonnement par récurrence : Récurrence simple

Question

En combien de mouvements au minimum est-il possible de résoudre le problème de la tour de Hanoï (amener tous les disques sur le poteau de droite) à 4 disques ?

Règles :

- Un seul disque bouge à la fois
- Un disque ne peut pas être au-dessus d'un disque de plus petit diamètre

Raisonnement par récurrence : Récurrence simple

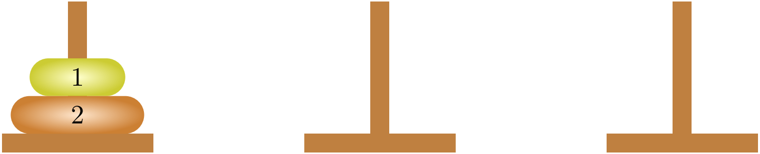
Question

En combien de mouvements au minimum est-il possible de résoudre le problème de la tour de Hanoï (amener tous les disques sur le poteau de droite) à ~~4~~ 3 disques ?

Règles :

- Un seul disque bouge à la fois
- Un disque ne peut pas être au-dessus d'un disque de plus petit diamètre

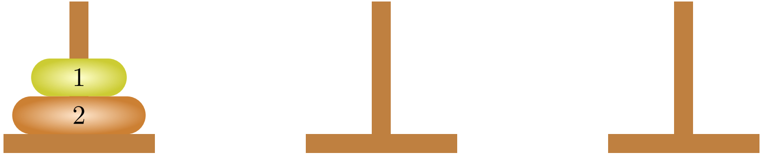
Raisonnement par récurrence : Récurrence simple



Question

En combien de mouvements au minimum est-il possible de résoudre le problème de la tour de Hanoï (amener tous les disques sur le poteau de droite) à ~~3~~ 2 disques ?

Raisonnement par récurrence : Récurrence simple



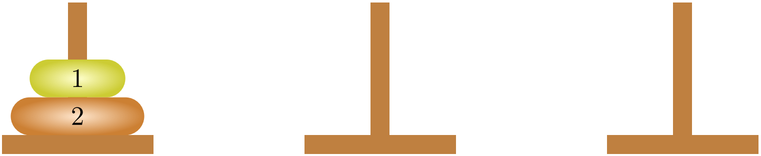
Question

En combien de mouvements au minimum est-il possible de résoudre le problème de la tour de Hanoï (amener tous les disques sur le poteau de droite) à ~~3~~ 2 disques ?

Réponse

3 !

Raisonnement par récurrence : Récurrence simple



Question

En combien de mouvements au minimum est-il possible de résoudre le problème de la tour de Hanoï (amener tous les disques sur le poteau de droite) à ~~3~~ 2 disques ?

Réponse

$3\,!(=:a_2)$

Raisonnement par récurrence : Récurrence simple

Question

En combien de mouvements au minimum est-il possible de résoudre le problème de la tour de Hanoï (amener tous les disques sur le poteau de droite) à 3 disques ?

Raisonnement par récurrence : Récurrence simple

Question

En combien de mouvements au minimum est-il possible de résoudre le problème de la tour de Hanoï (amener tous les disques sur le poteau de droite) à 3 disques ?

Réponse

$$a_3 = 2a_2 + 1 = 2 \times 3 + 1 = 7 = 8 - 1$$

Raisonnement par récurrence : Récurrence simple

Question

En combien de mouvements au minimum est-il possible de résoudre le problème de la tour de Hanoï (amener tous les disques sur le poteau de droite) à n disques ?

Raisonnement par récurrence : Récurrence simple

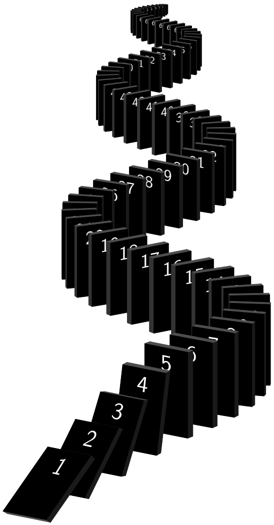
Question

En combien de mouvements au minimum est-il possible de résoudre le problème de la tour de Hanoï (amener tous les disques sur le poteau de droite) à n disques ?

Réponse

$$a_n = 2a_{n-1} + 1 = 2^n - 1$$

Raisonnement par récurrence : Récurrence simple



Raisonnement par récurrence : Récurrence simple

Soit $\mathcal{P}(n)$, la propriété à prouver pour tout entier $n \geq n_0$.

Deux étapes :

- Initialisation / cas de base
- Hérédité / cas inductif

- Initialisation : Montrer $\mathcal{P}(n_0)$
- Hérédité : Pour $k \geq n_0$, montrer $\mathcal{P}(k+1)$ en supposant $\mathcal{P}(k)$

Conclusion : $\mathcal{P}(n)$ vraie pour tout $n \geq n_0$

Raisonnement par récurrence : Récurrence forte

Soit $\mathcal{P}(n)$, la propriété à prouver pour tout entier $n \geq n_0$.

Deux étapes :

- Initialisation
- Hérédité (forte !)

- Initialisation : Montrer $\mathcal{P}(n_0)$
- Hérédité : Pour $k \geq n_0$, montrer $\mathcal{P}(k+1)$ en supposant $\mathcal{P}(k), \mathcal{P}(k-2), \ldots, \mathcal{P}(n_0)$

Conclusion : $\mathcal{P}(n)$ vraie pour tout $n \geq n_0$

Exemple

- Algorithme de tri (par exemple, tri fusion)
- Mq tout entier $n > 0$ admet une expression binaire (càd qu'il existe $c_i \in \{0;1\}$ tq $n = c_r 2^r + c_{r-1} 2^{r-1} + \ldots + c_0 2^0$)

À vous !

Exercice(s)

Exercices 5 et 6 de la feuille de TD3

Exemple

Le code suivant est-il correct ? Pourquoi ?

Définition inductive

Définition

Une définition inductive d'un ensemble d'objets O est donnée par :

- des éléments initiaux,
- des constructeurs (=application $O^k \to O$, $k \geq 1$).

Définition inductive

Définition

Une définition inductive d'un ensemble d'objets O est donnée par :

- des éléments initiaux,
- des constructeurs (=application $O^k \to O$, $k \geq 1$).

Exemple

Les entiers naturels sont définis comme :

- un élément 0
- un constructeur succ qui associe à un entier naturel son successeur

$$\mathbb{N} = \{0\} \cup \{\mathbb{N}\}$$

Définition inductive

Exemple

L'ensemble des mots $\mathcal{M}$ sur un ensemble fini $\mathcal{A}$ est défini comme :

- un élément de $\mathcal{A}$,
- un constructeur qui associe à une paire formée d'un élément de $\mathcal{A}$ et d'un élément de $\mathcal{M}$ le mot obtenu par concaténation.

$$\mathcal{M} = \mathcal{A} \cup (\mathcal{A} \times \mathcal{M})$$

Définition inductive

Exemple

L'ensemble des mots $\mathcal{M}$ sur un ensemble fini $\mathcal{A}$ est défini comme :

- un élément de $\mathcal{A}$,
- un constructeur qui associe à une paire formée d'un élément de $\mathcal{A}$ et d'un élément de $\mathcal{M}$ le mot obtenu par concaténation.

$$\mathcal{M} = \mathcal{A} \cup (\mathcal{A} \times \mathcal{M})$$

Exemple

L'ensemble des formules logique $\mathcal{L}$ sur un ensemble fini de variables propositionnelles $\mathcal{P}_0$ est défini comme :

- une variable propositionnelle,
- trois constructeurs $\neg : \mathcal{L} \to \mathcal{L}$, $\vee : \mathcal{L} \times \mathcal{L} \to \mathcal{L}$ et $\wedge : \mathcal{L} \times \mathcal{L} \to \mathcal{L}$.

Définition inductive

Exemple

Considérons la structure I définie comme :

- un élément $\emptyset$
- un constructeur qui associe à une paire d'éléments de I (i_g, i_d) l'élément $\{\bullet, i_g, i_d\}$

$$I = \{\emptyset\} \cup (\{\bullet\} \times I \times I)$$

Question

À quelle structure cette définition correspond-t-elle ?

Lien avec le cardinal de l'ensemble défini inductivement

Souvenez-vous, $\cup = +$ et $\times = \cdot$!
Le nombre de mots sur l'alphabet $\mathcal{A}$ est alors donné par :

$$|\mathcal{M}| = |\mathcal{A}| + (|\mathcal{A}| \times |\mathcal{M}|)$$

Lien avec le cardinal de l'ensemble défini inductivement

Souvenez-vous, $\cup = +$ et $\times = \cdot$!
Le nombre de mots sur l'alphabet $\mathcal{A}$ est alors donné par :

$$|\mathcal{M}| = |\mathcal{A}| + (|\mathcal{A}| \times |\mathcal{M}|)$$

Attention

$\mathcal{M}$ n'est pas fini !

Lien avec le cardinal de l'ensemble défini inductivement

Notant m_n l'ensemble des mots obtenus en appliquant au plus $n-1$ fois un constructeur, l'équation

$$\mathcal{M} = \mathcal{A} \cup (\mathcal{A} \times \mathcal{M})$$

devient

$$m_1 = |\mathcal{A}|$$

et

$$m_n = |\mathcal{A}| \cdot m_{n-1}$$

Raisonnement par induction structurelle

Question

Comment montrer une propriété sur de tels objets définis récursivement ?

Raisonnement par induction structurelle

Question

Comment montrer une propriété sur de tels objets définis récursivement ?

Souvenez-vous, pour une récurrence normale :

Deux étapes :

- Initialisation / cas de base
- Hérédité / cas d'induction

Raisonnement par induction structurelle

Question

Comment montrer une propriété sur de tels objets définis récursivement ?

Ici :

Deux étapes :

- Initialisation $\rightarrow$ montrer que la propriété est vraie pour les éléments initiaux
- Hérédité $\rightarrow$ Pour tout constructeur $f : E^k \rightarrow E$, montrer que si la propriété est vrai pour des éléments $x_1, \ldots, x_k$, alors elle l'est aussi pour $f(x_1, \ldots, x_k)$

Raisonnement par induction structurelle

Deux étapes :

- Initialisation $\rightarrow$ montrer que la propriété est vraie pour les éléments initiaux
- Hérédité $\rightarrow$ Pour tout constructeur $f : E^k \rightarrow E$, montrer que si la propriété est vrai pour des éléments $x_1, \ldots, x_k$, alors elle l'est aussi pour $f(x_1, \ldots, x_k)$

Exemple

Pour les entiers, l'élément initial est 0 et l'unique constructeur est succ : $n \mapsto n+1$:on retrouve la récurrence simple.

À vous !

Exercice(s)

Exercices 2 et 3 de la feuille de TD3

Exercice(s)

Soit a un arbre binaire et soit P la propriété suivante :

$$P(a) \text{ ssi } |\text{feuilles}(a)| = |\text{noeuds internes}(a)| + 1$$

Démontrer par induction la propriété P pour tout les arbres binaires.

Exercice(s)

Exercice 4 de la feuille de TD3

Marches et chemins

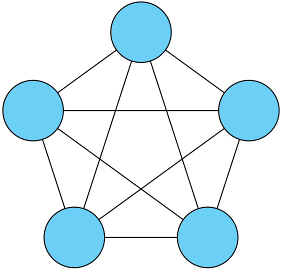
Définition

Une marche sur un graphe $G = (V, E)$ est une liste de sommets

$$(v_0, v_1, \ldots, v_t)$$

où $v_i \in V$ et deux sommets consécutifs de la listes sont voisins.
t est alors la longueur de la marche. Un chemin est une marche dont tous les sommets sont distincts.
Un cycle est une marche qui revient à son point de départ ($v_t = v_0$), et telle que $(v_0, v_1, \ldots, v_{t-1})$ soit un chemin.

Marches et chemins



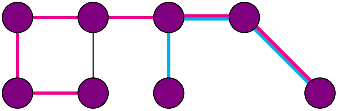
Maximalité et longueur

Considérons un graphe $G = (V, E)$.

Définition

Un chemin maximal de G est un chemin $(v_0, \ldots, v_n)$ qui ne peut pas être prolongé en un chemin $(v_0, \ldots, v_n, v_{n+1})$, càd qu'il n'existe pas de sommet v_{n+1} tel que la marche $(v_0, \ldots, v_n, v_{n+1})$ soit un chemin. (-)

Un chemin de longueur maximale est un chemin $(v_0, \ldots, v_n)$ tel qu'il n'existe aucun chemin $(v'_0, \ldots, v'_n, v'_{n+1})$. Un chemin de longueur maximal est notamment un chemin maximal. (-)



À vous !

Exercice(s)

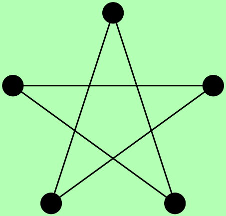
Exercice 3 de la feuille de TD3

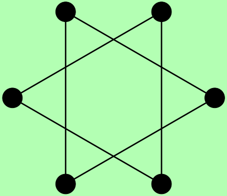
Connexité

Définition

Un graphe est connexe si pour tous sommets $x, y \in V(G)$, il existe une marche de x à y. Dans ce cas, il existe aussi un chemin de x à y.

Exemples



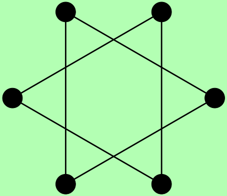


Composante connexe

Définition

Une composante connexe d'un graphe est un sous-graphe connexe maximal.

Exemple

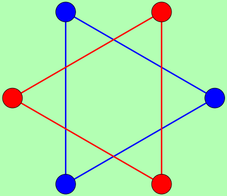


Composante connexe

Définition

Une composante connexe d'un graphe est un sous-graphe connexe maximal.

Exemple



Un peu de pratique

Exercice(s)

Exercices 1 à 5 de la feuille de TD 3.

Acyclicité

Définition

Un graphe est acyclique s'il n'existe aucun cycle dans le graphe

Proposition

Un graphe G est acyclique si et seulement si pour tous sommets u et v de G, il existe au plus un chemin entre u et v.

Exercice(s)

Exercice 6 de la feuille de TD 3

Propriété des graphes acycliques

Proposition (ex6 TD3)

Tout graphe acyclique sur n *sommets a au plus* $n-1$ *arêtes. Plus précisément, un graphe acyclique à* k *composantes connexes a* $n-k$ *arêtes pour tout* $0 < k \leq n$*.*

Question

Qu'est-ce qu'un graphe qui est à la fois acyclique et connexe ?

Qu'est-ce qu'un arbre ?

Définition

Un arbre est un graphe connexe et acyclique (=sans cycle).

Théorème (Exercice 8 du TD 3)

Les conditions suivantes sont équivalentes :

1. G *est un arbre*
2. *Entre tous sommets* x *et* y*, il existe un et un seul chemin*
3. *Le graphe est connexe et enlever une arête (n'importe laquelle) déconnecte le graphe (connexité minimale)*
4. *Le graphe est acyclique et ajouter n'importe quelle arête forme un cycle (acyclicité maximale)*
5. G *est connexe et* $|E| = |V| - 1$
6. G *est acyclique et* $|E| = |V| - 1$

Propriétés des arbres

Définition

Une feuille est un sommet de degré 1. Les autres sommets sont appelés nœuds.

Lemme

Tout arbre, sur au moins deux sommets, possède au moins deux feuilles

Lemme

Pour G un graphe et v une feuille de G, G est un arbre si et seulement si $G - \{v\}$ est un arbre.

Un peu de pratique

Exercice(s)

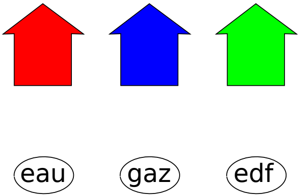
Ex 7 et 8 de la feuille de TD 3

Fin de la premiere partie du cours

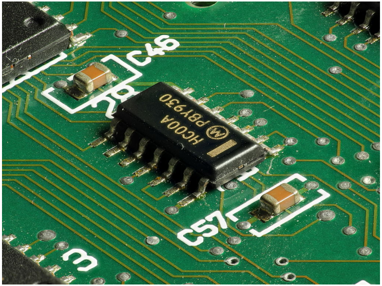
Problème des trois fournisseurs

Question

Trois fournisseurs d'eau, gaz et électricité veulent relier trois maisons aux réseaux existants. Le sol étant peu profond, il faudrait que les canalisations tiennent dans un plan. Est-ce possible ?



Comment fabriquer un circuit imprimé ?



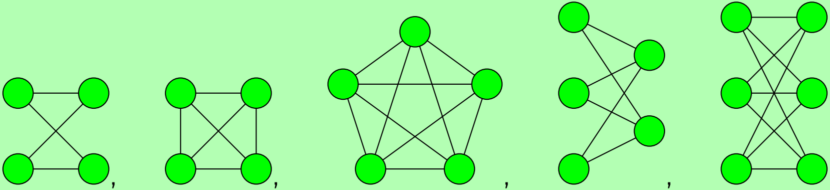
Graphes planaires

Définition

Un graphe planaire est un graphe qui possède une représentation dans le plan dans laquelle deux arêtes ne se coupent jamais

Exemples

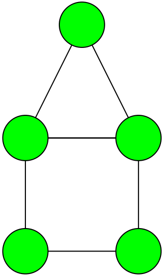
Les graphes suivants sont-ils planaires ?



Face d'un graphe planaire

Définition

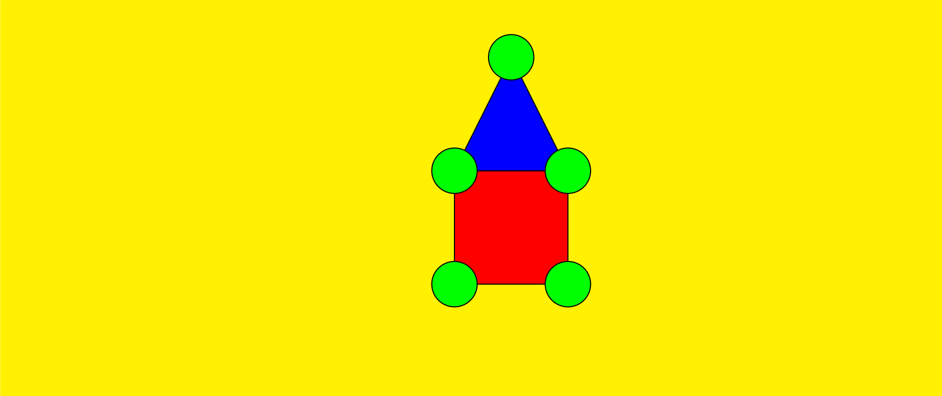
Une face d'un graphe planaire est une zone du plan délimitée par des arêtes qui l'entourent et ne contenant pas elle-même d'arêtes. (On peut déterminer sa délimitation en imaginant un personnage qui suivrait les bords des arêtes jusqu'à revenir à son point de départ)



Face d'un graphe planaire

Définition

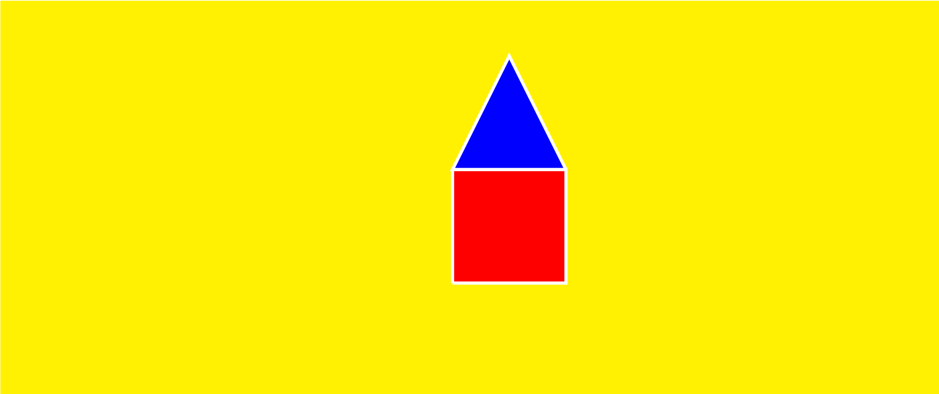
Une face d'un graphe planaire est une zone du plan délimitée par des arêtes qui l'entourent et ne contenant pas elle-même d'arêtes. (On peut déterminer sa délimitation en imaginant un personnage qui suivrait les bords des arêtes jusqu'à revenir à son point de départ)



Face d'un graphe planaire

Définition

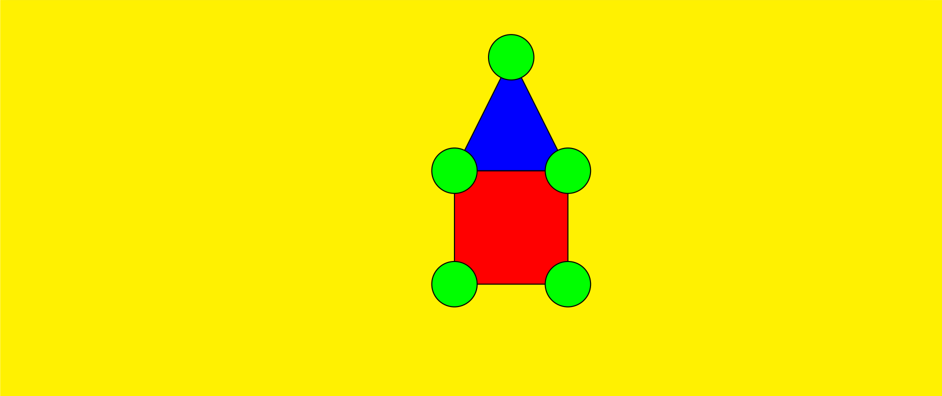
Une face d'un graphe planaire est une zone du plan délimitée par des arêtes qui l'entourent et ne contenant pas elle-même d'arêtes. (On peut déterminer sa délimitation en imaginant un personnage qui suivrait les bords des arêtes jusqu'à revenir à son point de départ)



Face d'un graphe planaire

Définition

Une face d'un graphe planaire est une zone du plan délimitée par des arêtes qui l'entourent et ne contenant pas elle-même d'arêtes. (On peut déterminer sa délimitation en imaginant un personnage qui suivrait les bords des arêtes jusqu'à revenir à son point de départ)



Formule d'Euler

Théorème (Formule d'Euler)

Tout graphe planaire connexe vérifie :

$$n - a + f = 2,$$

avec n le nombre de sommets,
a le nombre d'arêtes
et f le nombre de faces du graphe (dans une de ses représentations planaires).

Démonstration.

Preuve par récurrence $\square$

Formule d'Euler

Théorème (Formule d'Euler)

Tout graphe planaire connexe vérifie $n - a + f = 2$, avec n le nombre de sommets, a le nombre d'arêtes et f le nombre de faces du graphe (dans une de ses représentations planaires).

Démonstration.

Preuve par récurrence sur le nombre d'arêtes du graphe. **Initialisation :** Si $a = 0$, un seul graphe connexe est possible, le sommet isolé.
$a = 0, n = 1, f = 1$ et on a bien $1 - 0 + 1 = 2$.
Hérédité Soit G un graphe connexe avec a arêtes.
Cas 1 : G a un cycle. Retirer une arête u, v d'un cycle de G. G' reste connexe car il existe un (autre) chemin de u à v dans G. Le cycle formait une face et chaque arête est adjacente à 2 faces donc G' a $f - 1$ faces, $a - 1$ arêtes, et n sommets. Par hypothèse de récurrence,
$2 = n - (a - 1) + (f - 1) = n - a + f$.

□

Formule d'Euler

Théorème (Formule d'Euler)

Tout graphe planaire connexe vérifie $n-a+f=2$, avec n le nombre de sommets, a le nombre d'arêtes et f le nombre de faces du graphe (dans une de ses représentations planaires).

Démonstration.

Preuve par récurrence sur le nombre d'arêtes du graphe.
Cas 2 : G n'a pas de cycle donc $f=1$. Retirer une arête de G déconnecte G en 2 composantes connexes G' et G''. Appelons a' le nombre d'arêtes et n' le nombre de sommets de G', et de même pour a'' et n'' pour G''. On a que $n'+n''=n$, et $a'+a''=a-1$. G' et G'' ont une face car ils ne contiennent pas de cycle. En appliquant l'hypothèse d'induction à G' et G'' on obtient $n'-a'+1=2$ et $n''-a''+1=2$. Sommant les deux, $4=(n'+n'')-(a'+a'')+2=n-(a-1)+2$ donc $2=n-a+f$ car $f=1$.

$\square$

Formule d'Euler

Théorème (Formule d'Euler)

Tout graphe planaire connexe vérifie :

$$n - a + f = 2,$$

avec n le nombre de sommets,
a le nombre d'arêtes
et f le nombre de faces du graphe (dans une de ses représentations planaires).

Question

Que donne cette formule appliquée aux exemples précédents ?

Un peu de pratique

Exercice(s)

Exercices 1 et 2 de la feuille de TD 4

Exercices 3-5 de la feuille de TD4

Critères de graphes planaires

Proposition

Dans un graphe connexe planaire, le nombre d'arêtes a et le nombre de sommets n vérifie :

$$a \leq 3n - 6$$

Si, de plus, le graphe est sans triangle, on a :

$$a \leq 2n - 4$$

Théorème de Kuratowski

Théorème

Un graphe fini est planaire ssi il ne contient aucun sous-graphe qui est une subdivision de K_5 ou $K_{3,3}$.

Une subdivision d'un graphe est obtenue en insérant des sommets au milieu d'arêtes.

Graphes bipartis

Définition

Un graphe biparti est un graphe non orienté (V, E) où

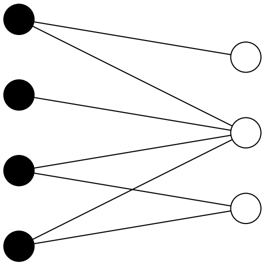
- l'ensemble des sommets V se scinde en deux sous-ensembles distincts $V = V_b \sqcup V_n$, les éléments de V_b sont les sommets blancs et ceux de V_n sont les sommets noirs,
- toute arête de E a un élément dans V_b et un élément dans V_n. E est donc un ensemble de paires d'un sommet de V_b et d'un sommet de V_n.

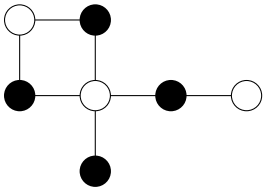
Graphes bipartis

Définition

Un graphe biparti est un graphe non orienté (V, E) où

- l'ensemble des sommets V se scinde en deux sous-ensembles distincts $V = V_b \sqcup V_n$, les éléments de V_b sont les sommets blancs et ceux de V_n sont les sommets noirs,
- toute arête de E a un élément dans V_b et un élément dans V_n. E est donc un ensemble de paires d'un sommet de V_b et d'un sommet de V_n.





Graphes bipartis

Définition

Un graphe biparti est un graphe non orienté (V, E) où

- l'ensemble des sommets V se scinde en deux sous-ensembles distincts $V = V_b \sqcup V_n$, les éléments de V_b sont les sommets blancs et ceux de V_n sont les sommets noirs,
- toute arête de E a un élément dans V_b et un élément dans V_n. E est donc un ensemble de paires d'un sommet de V_b et d'un sommet de V_n.

Question

Les graphes complets sont-ils bipartis ?

Graphes bipartis

Proposition

Un graphe est biparti si et seulement s'il ne contient aucun cycle de longueur impair.

Exercice(s)

Exercice 6 de la feuille de TD 4

1. Probabilités discrètes
   - Espace de probabilité
   - Probabilité conditionnelle
   - Indépendance
   - Variables aléatoires et Espérance

Motivation

En informatique

- les données peuvent être aléatoires ou bruitées
- les algorithmes peuvent être probabilistes (Ex. test de primalité)
- les pannes sont imprévisibles

On souhaite avoir des algorithmes efficaces (pour des données typiques), résistants (aux pannes aléatoires), corrects (presque corrects, presque toujours),...

Dénombrement et probabilité

Exemple

Un algorithme trouve votre mot de passe une fois sur deux.

- Si on exécute l'algorithme 3 fois, combien de résultats sont possibles ?
- Quel est le pourcentage de chances de trouver votre mot de passe ?

Exemple

Un algorithme choisit au hasard 3 sommets d'un graphe et répond Vrai si les 3 sommets forment un triangle.

- Combien y a-t-il d'exécutions possibles ?
- Si le graphe est complet, quelle est la probabilité de trouver un triangle ? Si le graphe est biparti ? Si le graphe contient un unique triangle ?

Dénombrement et probabilité

Exemple

Considérant une famille qui a au plus trois enfants :

- Combien y a-t-il de fratries possibles ?
- Combien y a-t-il de fratries avec au moins un garçon et au moins une fille ? FG, GF, FFG, FGF, GFF, FGG, GFG, GGF -> 8
- Quel est le pourcentage des familles à au plus trois enfants qui ont au moins un garçon et au moins une fille ? Conclusion : plus de la moitié des familles vérifient ça !

Tirages, événements

Un tirage consiste à prendre un élément au hasard dans un ensemble fini Ω, appelé univers. Un évènement concerne une propriété de l'élément choisi.

Exemple

Il y a 3 dragibus roses, 4 dragibus verts et 5 dragibus bleus dans un sac. Alice aime uniquement les dragibus verts. Quelle est la probabilité qu'elle en obtienne un si elle tire un bonbon au hasard ?

Si B représente l'ensemble des bonbons, V représente l'ensemble des dragibus verts, et x est le bonbon tiré par Alice alors l'événement "Alice a tiré un dragibus verts" se traduit par "$x \in V$". On identifie cet évènement à l'ensemble V. Sa probabilité est $\mathbb{P}(V) = \frac{|V|}{|B|}$.

Tirages, événements

Exemple

Il y a 3 dragibus roses, 4 dragibus verts et 5 dragibus bleus dans un sac. Alice aime uniquement les dragibus verts et les roses. Quelle est la probabilité qu'elle en ait un si elle tire un bonbon au hasard ?

Si V représente l'ensemble des dragibus verts, R l'ensemble des dragibus roses, et x est le bonbon tiré par Alice alors l'événement "Alice a tiré un dragibus vert ou rose" se traduit par "$x \in V$ ou $x \in R$" ce qui revient à dire "$x \in V \cup R$". Sa probabilité est $\mathbb{P}(V \cup R) = \frac{|V \cup R|}{|B|}$.

Tirages, événements

Exemple

Il y a 6 couleurs différentes de dragibus, 4 de chaque couleur dans un sac. Alice aime tous les dragibus sauf les bleus. Quelle est la probabilité qu'elle en ait tiré un qu'elle aime un si elle tire un bonbon au hasard ?

Si N représente l'ensemble des dragibus bleus, et x est le bonbon tiré par Alice alors l'événement "Alice n'a pas tiré un dragibus bleu" se traduit par "$x \notin N$" ce qui revient à dire "$x \in B \setminus N$". Sa probabilité est $\mathbb{P}(\overline{N}) = \frac{|B|-|N|}{|B|}$.
Attention : on a supposé que chaque bonbon avait la même probabilité d'être tiré !

Espaces et univers

Définition

Un espace de probabilité (ou espace probabilisé) est un couple $(\Omega, \mathbb{P})$.

- L'ensemble fini (ou discret) Ω est appelé univers.
- Les éléments de Ω sont appelés évènements élémentaires.
- L'application $\mathbb{P} : \Omega \to [0,1]$ de probabilité est telle que :

$$\sum_{x \in \Omega} \mathbb{P}(x) = 1$$

- Un sous-ensemble $A \subseteq \Omega$ est un évènement et sa probabilité est

$$\mathbb{P}(A) = \sum_{x \in A} \mathbb{P}(x).$$

Exemples

lancers de un dé, de deux dés, prélèvement de deux boules dans une urne ...

Pour s'échauffer

Exercice(s)

Exercices 1 à 3 de la feuille de TD5

Tirages indépendants

Un tirage peut être composé de plusieurs tirages indépendants. Par exemple, on tire un dé deux fois, on répète un algorithme 2 fois, etc.
Si on tire un élément dans $(\Omega, \mathbb{P})$ et on tire indépendamment un élément dans $(\Omega', \mathbb{P}')$, alors la distribution jointe sera un tirage dans $(\Omega \times \Omega', \mathbb{P} \cdot \mathbb{P}')$.

Exemple

On tire à pile ou face avec une pièce non-biaisée. L'univers $\Omega = \{P, F\}$ et $\mathbb{P}(P) = \mathbb{P}(F) = \frac{1}{2}$. Si on effectue 2 tirages successifs de façon indépendantes, l'univers est

$$\{P, F\} \times \{P, F\} = \{(P, P), (P, F), (F, P), (F, F)\}.$$

La probabilité de (P, P) est

$$\mathbb{P}(P) \cdot \mathbb{P}(P) = \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}.$$

Probabilité uniforme

Définition

Une probabilité est dite uniforme quand pour tout évènement élémentaire $\omega \in \Omega$, on a :

$$\mathbb{P}(\omega) = \frac{1}{|\Omega|}$$

Exemple

Probabilité uniforme : Lancer d'un dé cubique équilibré. Lancer de 2 pièces équilibrées.

Probabilité non-uniforme : Une urne contient 3 boules rouges et 3 boules bleues. On tire 2 boules au hasard, sans remise. Quelle est la probabilité de tirer 2 boules bleues ? Quelle est la probabilité de tirer une bleue et une rouge (dans cet ordre) ?

Probabilité non-uniforme

Exemple

Un algorithme trouve votre mot de passe une fois sur trois.

- Si on exécute l'algorithme 3 fois, quels sont les huit évènements élémentaires ?
- Quelle est la probabilité de chaque événement élémentaire ?
- A quel ensemble d'événements élémentaires correspond l'événement "le mot de passe a été trouvé" ?
- Quelle est la probabilité de trouver votre mot de passe ?

Propriété des probabilités

Proposition

- $\mathbb{P}(A \cup B) = \mathbb{P}(A) + \mathbb{P}(B) - \mathbb{P}(A \cap B)$ *(principe d'inclusion exclusion)*
- $\mathbb{P}(A \cup A^c) = 1$
- *Si* $A \subseteq B$, $\mathbb{P}(A) \leq \mathbb{P}(B)$.

Exemple

Un dé rouge et un dé vert sont lancés, quelle est la probabilité que l'un des deux dés donne un 2 ?

Propriété des probabilités

Proposition

- $\mathbb{P}(A \cup B) = \mathbb{P}(A) + \mathbb{P}(B) - \mathbb{P}(A \cap B)$ *(principe d'inclusion exclusion)*
- $\mathbb{P}(A \cup A^c) = 1$
- *Si* $A \subseteq B$, $\mathbb{P}(A) \leq \mathbb{P}(B)$.

Exemple

Un dé rouge et un dé vert sont lancés, quelle est la probabilité que l'un des deux dés donne un 2 ?

$$\begin{aligned} P(R2 \cup G2) &= P(R2) + P(G2) - P(R2 \cap G2) \\ &= \frac{1}{6} + \frac{1}{6} - \frac{1}{36} \\ &= \frac{11}{36} \end{aligned}$$

Propriété des probabilités

Proposition

- $\mathbb{P}(A \cup B) = \mathbb{P}(A) + \mathbb{P}(B) - \mathbb{P}(A \cap B)$ *(principe d'inclusion exclusion)*
- $\mathbb{P}(A \cup A^c) = 1$
- *Si* $A \subseteq B$, $\mathbb{P}(A) \leq \mathbb{P}(B)$.

Exemple

- Quelle est la probabilité que lors du lancer d'un dé, le dé donne 1 ou un nombre strictement plus grand que 1 ?
- Lors du lancer d'un dé, que dire de la probabilité d'obtenir un 2 par rapport à celle d'obtenir un nombre pair ?

Pour s'échauffer

Exercice(s)

Exercices 4 à 6 de la feuille de TD5

Pour aller plus loin : exercices 7 à 9 de la feuille de TD5

Parenthèse combinatoire : Principe d'inclusion-exclusion

Rappel

Soient A et B deux évènements.

$$\mathbb{P}(A \cup B) = \mathbb{P}(A) + \mathbb{P}(B) - \mathbb{P}(A \cap B)$$

Théorème

Soit $A_1, \ldots, A_n$ des ensembles. Le nombre d'éléments de $A_1 \cup \ldots \cup A_n$ est donné par :

$$\begin{aligned} |A_1 \cup \ldots \cup A_n| &= \sum_{i=1}^{n} |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| + \ldots + (-1)^{n-1} |A_1 \cap \ldots \cap A_{n-2}| \\ &= \sum_{k=1}^{n-1} (-1)^{k-1} \sum_{1 \leq i_1 < \ldots < i_k \leq n} |A_{i_1} \cap \ldots \cap A_{i_k}| \end{aligned}$$

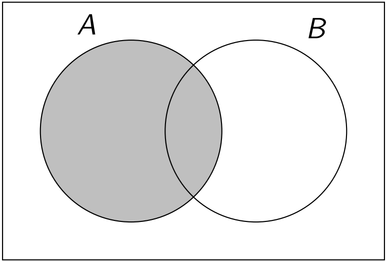
Pour s'échauffer

Exercice(s)

Exercice 10 de la feuille de TD 5

Probabilité conditionnelle

Étant donné deux événements A et B, la probabilité conditionnelle de B sachant A est la probabilité de B sachant que l'événement A est avéré.
Si A est avéré, l'univers des événements élémentaires qui restent possibles est limité à l'ensemble A.
La loi de probabilité sur l'univers réduit à l'ensemble A doit être *renormalisée* afin que les probabilités somment à 1. On calcule donc la probabilité de B, sachant A, par rapport à cette nouvelle distribution.



Loi de Bayes

Proposition

Si $\mathbb{P}(B) \neq 0$*, la* *probabilité conditionnelle* *de* B *sachant* A *est donnée par :*

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

ou de façon équivalente :

$$\mathbb{P}(A \cap B) = \mathbb{P}(A) \cdot P(B|A).$$

"Choisir A et B revient à choisir A, puis choisir B sachant que A s'est produit"

Indépendance

Soient A et B deux événements sur un même espace de probabilité $(\Omega, \mathbb{P})$. Intuitivement deux événements sont indépendants si l'un n'influence pas la probabilité de l'autre.

Exemple

On lance un dé. L'événement "le résultat est pair" et l'événement "le résultat est 4" ne sont PAS indépendants !

Indépendance

Définition

Si $\mathbb{P}(B) \neq 0$, A et B sont indépendants si et seulement si

$$\mathbb{P}(A|B) = \mathbb{P}(A).$$

Proposition

A et B sont indépendants si et seulement si

$$\mathbb{P}(A \cap B) = \mathbb{P}(A) \cdot \mathbb{P}(B).$$

Indépendance

Exemple

On lance onze fois de suite une pièce équilibrée. Que dire des événements

- A = “le résultat des 10 premiers lancers est face” et
- B =“le onzième lancer donne face”?

Indépendance

Exemple

On lance 2 dés. On considère trois événements.

- A = “Le premier est un 2”
- B = “Le second est un 5”
- C = “La somme des dés est 7.”

Quelles sont les paires d’événements indépendants ?
Pensez-vous que les 3 événements sont indépendants ?

Indépendance

Soient $A_1, \ldots, A_k$, k événements.

Définition

Les A_k sont indépendants si et seulement si

$$\mathbb{P}(A_{i_1} \cap \ldots \cap A_{i_p}) = \prod_{j=1}^{p} \mathbb{P}(A_{i_j}),$$

pour tout $\{i_1, \ldots, i_p\} \subseteq \{1, \ldots, k\}$, $i_1 < i_2 < \ldots < i_p$.

Attention

Parfois il faut conditionner sur plusieurs événements pour voir apparaître un effet sur la probabilité conditionnelle d'un autre événement. (voir TD 5 Exercice 13 pour autre exemple)

Pour s'échauffer

Exercice(s)

Exercices 11 à 14 de la feuille de TD 5

Probabilités conditionnelles et indépendance

Exemple

Supposons que quatre pièces équilibrées sont lancées. Considérons les trois événements suivants
A="Au moins deux pièces sont côté face",
B="Au plus deux pièces sont côté face"
et C="Exactement deux pièces sont côté face".
Calculez :

1. $\mathbb{P}(A)$
2. $\mathbb{P}(B)$
3. $\mathbb{P}(C)$
4. $\mathbb{P}(A|B)$
5. $\mathbb{P}(A|C)$
6. $\mathbb{P}(A \cup B)$

Bonus : Indépendance vs disjonction

Attention

Différence entre indépendance et disjonction ! !

Considérons un jeu de 52 cartes dans lequel on tire au hasard une carte.
K="cette carte est un roi"
T="cette carte est un trèfle"
Q="cette carte est une reine"

Question

- K et T sont-ils indépendants ? disjoints ?
- Q et T sont-ils indépendants ? disjoints ?

exemple d'événements indépendants et disjoints ? il faut que l'un des deux soit trivial

Bonus : Indépendance vs disjonction

Attention

Différence entre indépendance et disjonction ! !

Considérons un jeu de 52 cartes dans lequel on tire au hasard une carte.
K="cette carte est un roi"
T="cette carte est un trèfle"
Q="cette carte est une reine"

Question

- K et T sont-ils indépendants ? disjoints ?
- Q et T sont-ils indépendants ? disjoints ?

Réponse

K et T sont indépendants mais non disjoints et K et Q sont disjoints mais non indépendants.

exemple d'événements indépendants et disjoints ? il faut que l'un des deux

Variable aléatoire

On peut associer une valeur aux événements élémentaires.

Définition

Une variable aléatoire est une application de Ω dans $\mathbb{R}$ (souvent dans $\mathbb{N}$).

Soit X une variable aléatoire. On associe au prédicat "$X = v$" l'ensemble d'événements élémentaires correspondant : $X^{-1}(v) = \{\omega \in \Omega | X(\omega) = v\}$.

Notation

Nous écrirons $\mathbb{P}(X = v)$ pour la probabilité de l'événement associé $\mathbb{P}(X^{-1}(v))$.

Exemple

À une expérience de lancer successif de deux dés, on peut associer les variables aléatoires suivantes, pour w le résultat des deux lancers :
$S(w) =$ somme des points sur le dessus du dé
$P(w) =$ produit des points sur le dessus du dé

Espérance (=comportement moyen)

Définition

La *valeur moyenne*, ou *espérance*, d'une variable aléatoire X est définie par

$$\mathbb{E}(X) = \sum_{\omega \in \Omega} \mathbb{P}(\omega) \cdot X(\omega).$$

Proposition

Si X et Y sont deux variables aléatoires,

$$\mathbb{E}(X+Y) = \mathbb{E}(X) + \mathbb{E}(Y).$$

Plus généralement, l'espérance est linéaire, c'est-à-dire que pour tout α, β,

$$\mathbb{E}(\alpha X + \beta Y) = \alpha \mathbb{E}(X) + \beta \mathbb{E}(Y).$$

Espérance

Exemple

- $\mathbb{E}(S)$
- $\mathbb{E}(\mathbb{1}_A)$ pour $A \in \Omega$ et $\mathbb{1}_A$ la variable aléatoire qui vaut 1 sur les événements élémentaires $\omega \in A$ et 0 sinon.
- ...

Indépendance des variables aléatoires

Définition

Si les variables ne prennent que des valeurs entières positives, les variables aléatoires X et Y sont indépendantes si et seulement si pour tout couple (m, n) de nombres naturels,

$$\mathbb{P}((X = m) \cap (Y = n)) = \mathbb{P}(X = m) \cdot \mathbb{P}(Y = n).$$

Exemple

Les variables aléatoires S et P sont-elles indépendantes ?

Espérance

Proposition

Si X et Y sont deux v.a. sur le même espace de probabilité, on a :

$$\mathbb{E}(X+Y) = \mathbb{E}(X) + \mathbb{E}(Y).$$

Plus généralment, l'espérance est linéaire, c'est-à-dire que pour tout α, β,

$$\mathbb{E}(\alpha X + \beta Y) = \alpha \mathbb{E}(X) + \beta \mathbb{E}(Y).$$

De plus, si X et Y sont indépendantes,

$$\mathbb{E}(XY) = \mathbb{E}(X)\mathbb{E}(Y)$$

Exemple

Calculer $\mathbb{E}(P)$.
Considérons un lancer de dé, $X = \mathbb{1}_{\omega=1}$ et $Y = \mathbb{1}_{\omega=2}$, calculer $\mathbb{E}(XY)$, $\mathbb{E}(X)$ et $\mathbb{E}(Y)$.

Un peu de pratique

Exercice(s)

Exercices 1 à 4 de la feuille de TD6

Loi binomiale

On effectue n tirages indépendants d'une expérience qui réussit avec probabilité $1/2$ et échoue avec probabilité $1/2$. Soit X la variable aléatoire qui représente le nombre de succès obtenus sur les n tirages. Que vaut $\mathbb{P}(X = k)$?
Si maintenant on effectue n tirages indépendants d'une expérience qui réussit avec probabilité p, que vaut $\mathbb{P}(X = k)$?
On appelle cette loi la loi binomiale.
Rappel : Identité binomiale de Newton...

Inégalité de Markov

Soit X une variable aléatoire à valeurs positives et d'espérance E. Alors $\mathbb{P}(X > 3E) < \frac{1}{3}$.

Complexité en moyenne

Si un algorithme prend un temps $t(x)$ sur un exemplaire $x \in X$ et que l'exemplaire x se produit avec probabilité $p(x)$ alors la complexité en moyenne de l'algorithme sur les exemplaires X est $\sum_{x \in X} p(x)t(x)$.

Un peu de pratique

Exercice(s)

Exercice 5 à 8 de la feuille de TD6