Mathématiques discrètes
Polycopié d'exercices

Licence d'informatique deuxième année

2022-2023

Table des matières

1 Inductions sur les arbres binaires

Exercice 1 ★ Arbres binaires

1. Utilisez la définition inductive afin de lister tous les arbres binaires à 2 noeuds.
2. Même question avec 3 noeuds.
3. Pour chacun des arbres obtenus à la question précédente, on donnera le nombre de noeuds internes, le nombre de feuilles et la hauteur de l'arbre.

Exercice 2 ★ Relation entre la hauteur et le nombre de nœuds d'un arbre binaire
Soit A un arbre binaire, on notera $h(A)$ sa hauteur et $n(A)$ son nombre de nœuds.
Par convention, nous choisirons -1 comme hauteur de l'arbre vide.

1. Rappelez la définition inductive de la hauteur d'un arbre binaire.
2. Montrez par induction la propriété suivante :

$$h(A) + 1 \leq n(A)$$

3. Montrez par induction la propriété suivante :

$$n(A) \leq 2^{h(A)+1} - 1.$$

4. En déduire que pour tout arbre binaire A :

$$\log_2(n(A) + 1) - 1 \leq h(A) \leq n(A) - 1$$

Exercice 3 ★ Arbres binaires filiformes

1. Un arbre binaire dégénéré ou filiforme est un arbre de hauteur $n-1$ à n nœuds.
   Trouvez un shéma d'induction des arbres filiformes.
2. Listez les arbres filiformes à 3 noeuds.
3. Exprimez la hauteur des arbres binaires filiformes en fonction du nombre de noeuds. Comparer la à celle des arbres binaires.

Exercice 4 Arbres binaires complets
Un arbre binaire complet est un arbre binaire dont tous les niveaux sont complètement remplis. On suppose ici que l'arbre vide n'est pas complet.

1. Donnez un shéma d'induction de $\mathcal{C}$ où $\mathcal{C}$ est l'ensemble des arbres binaires complets.
2. Soit A un arbre binaire différent de l'arbre vide et A_g et A_d ses sous-arbres gauche et droit. Soit N un nœud de A, notons $p_A(N)$ la profondeur de N dans A. Si N est un nœud de A_g (resp A_d), donnez la relation entre $p_A(N)$ et $p_{A_g}(N)$ (resp $p_A(N)$ et $p_{A_d}(N)$).
3. Soit $k \in \mathbb{N}$ et A un arbre binaire. On considère la propriété $P_k(A)$: A possède soit 2^k nœuds de profondeur k soit aucun noeud de profondeur k.
   Montrez en utilisant les résultats des questions précédentes que l'on a :

$$\forall k \in \mathbb{N}\ \forall A \in \mathcal{C}\ P_k(A).$$

4. Combien de nœuds possède un arbre complet de hauteur h ?
5. Combien de feuilles possède un arbre complet de hauteur h ?

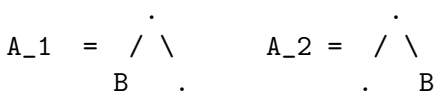
Exercice 5 ★ Arbres localement complets
Un arbre binaire est dit localement complet lorsqu'il n'est pas vide et que chaque nœud soit est une feuille, soit possède deux fils (c'est à dire que ses nœuds ont soit aucun soit deux fils.)

1. Donnez tous les arbres localement complets d'au plus 7 nœuds.
2. Donnez un schéma d'induction pour construire l'ensemble des arbres binaires localement complets.
3. Soit A un arbre binaire localement complet. Montrez par induction que A possède un nombre impair de nœuds.
4. Soit A un arbre binaire localement complet qui a $n = 2k + 1$ nœuds. Montrez par induction que A possède k nœuds internes et $k + 1$ feuilles.

Exercice 6 (CC-2018-2019)
On définit $\mathcal{P}$ sous-ensemble de l'ensemble des arbres binaires avec le schéma d'induction suivant :

(i) L'arbre réduit à une racine appartient à $\mathcal{P}$.

(ii) Soit B un arbre de $\mathcal{P}$. Les arbres A_1 et A_2 suivants appartiennent à $\mathcal{P}$:



Les arbres de $\mathcal{P}$ sont appelés des arbres peignes.

Soit A un arbre binaire. Nous noterons $h(A)$ la hauteur de A et $n_k(A)$ le nombre de nœuds de niveau (profondeur) k dans A. On définit, pour tout arbre binaire A, la propriété $P(A)$ suivante :
$P(A) : n_k(A) = 2$, pour tout $k \in \{1, \ldots, h(A)\}$.
Montrez par induction que $P(A)$ est vraie pour tout A de $\mathcal{P}$.

Exercice 7 Session1 2018-2019

1. Redonnez le schéma d'induction des arbres localement complets.
2. On définit une fonction f telle que $f(\cdot) = 1$ et, si $A = (\cdot, B, C)$ (A est constitué des deux sous-arbres B et C), alors $f(A) = 2\max(f(B), f(C))$.
   Montrez par induction sur les arbres localement complets que l'on a pour tout arbre localement complet A, $f(A) = 2^{h(A)}$, où $h(A)$ est la hauteur de A.

Exercice 8 Session2 2018-2019

1. Redonnez le schéma d'induction des arbres complets.
2. On attribue une valeur à chacun des nœuds des arbres non vides de la manière suivante :
   (i) Si A est l'arbre racine $\cdot$, alors la racine prend la valeur 1.
   (ii) Soit $A = (\cdot, B, C)$. Tous les nœuds de A différents de la racine conservent les valeurs de B ou C. La racine de A prend comme valeur la somme de la valeur de la racine de B et de celle de C.
   (a) Donnez les valeurs de nœuds de l'arbre complet de hauteur 3.
   (b) Montrez par induction que tout arbre complet non vide A a une racine de valeur $2^{h(A)}$.

Exercice 9 Arbres binaires et expressions
On considère des expressions arithmétiques avec les opérateurs binaires $+$ et $*$.
Soit $V = \{0, 1, 3, 4, 5, 6, 7, 8, 9\}$, on définit $\mathcal{E}$, l'ensemble des expressions arithmétiques, avec le schéma d'induction suivant :

i) Tous les éléments de V sont des expressions de $\mathcal{E}$.

ii) Si E_1 et E_2 sont des expressions de $\mathcal{E}$ alors $(E_1 + E_2)$ et $(E_1 * E_2)$ sont des expressions de $\mathcal{E}$.

1. Soit E une expression de $\mathcal{E}$. Nous noterons $N_+(E)$ (resp. $N_*(E)$, $N_v(E)$) le nombre d'occurrences de $+$ (resp. $*$, $v \in V$) dans E. Montrez par induction que toute expression E de $\mathcal{E}$ vérifie la relation
$$N_v(E) = N_+(E) + N_*(E) + 1.$$
2. Vérifier que les arbres sous-jacents aux expressions sont des arbres localement complets. La taille d'une expression est par définition $N(E) = N_v(E) + N_+(E) + N_*(E)$. Montrez qu'il y a autant d'arbres localement complets de taille $2k + 1$ que d'arbres binaires avec k nœuds.
3. Donnez un schéma d'induction des arbres complets.
Soit $h \in \mathbb{N}$, on considère une expression dont l'arbre sous-jacent est l'arbre complet de hauteur h. Donnez la taille de E. En déduire que toute expression de taille n correspond à un arbre d'une hauteur supérieure ou égale à $\log_2(n-1)$.

2 Ensembles

Exercice 10 ★ Parties d'un ensemble
Soient $S_1 = \{1, 2, 3, 4\}$ et $S_2 = \{1, \{2\}, \{3, 4\}\}$.
Déterminez $\mathcal{P}(S_1)$ et $\mathcal{P}(S_2)$.

Exercice 11 ★ Ensembles et grilles 2D
Soient $E = \{1, 2, 3, 4, 5\}$ et $F = \{2, 3, 4\}$ et $A = E \times E$.
On considère les sous-ensembles de A suivants :
$B = \{(i, i)/i \in E\}$, $C = \{(i, j)/i \in F, j \in E\}$, $D = \{(i, j)/i \in E, j \in F\}$
Représentez A par une grille et déterminer les ensembles $B \cap C$, $B \cap D$, $C \cap D$, $C \cup D$ et $C \Delta D$.

Exercice 12 ★
Soient A, B et C trois ensembles non vides tels que : $A \cap B \subset A \cap C$ et $A \cup B \subset A \cup C$.
Montrez que l'on a $B \subset C$.

Exercice 13 ★ Réunion et intersection des parties d'un ensemble
Soient E et F deux ensembles non vides. Laquelle des deux égalités suivantes est vérifiée ? On prouvera les inclusions qui sont vérifiées et on donnera un contre-exemple pour celles qui ne le sont pas.

1. $\mathcal{P}(E) \cup \mathcal{P}(F) = \mathcal{P}(E \cup F)$.
2. $\mathcal{P}(E) \cap \mathcal{P}(F) = \mathcal{P}(E \cap F)$.

Exercice 14 ★
Soient A, B, C,D des sous-ensembles non vides d'un ensemble E.

1. Comment est défini l'ensemble $A \setminus B$?
2. Montrez que $(A \setminus B) \setminus C = A \setminus (B \cup C)$.
3. Montrez que $A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C)$.
4. Montrez que $(A \setminus B) \cap (C \setminus D) = (A \cap C) \setminus (B \cup D)$.

Exercice 15 ★ Complémentaire d'un ensemble
Soit E un ensemble, A et B deux sous-ensembles non vides de E. On notera $\overline{A}$ le complémentaire de A dans E.

1. Montrez que $A \subset B$ implique $\overline{B} \subset \overline{A}$

2. Montrez les égalités $\overline{(A \cup B)} = \overline{A} \cap \overline{B}$ et $\overline{(A \cap B)} = \overline{A} \cup \overline{B}$
3. Soit A, B, C trois sous-ensembles non vides de E.
   On suppose que $\overline{A} \cap \overline{B} \subset \overline{A} \cap \overline{C}$ et $\overline{A} \cup \overline{B} \subset \overline{A} \cup \overline{C}$
   Montrez $C \subset B$. Indication : on pourra commencer par montrer que $\overline{B} \subset \overline{C}$.

Exercice 16 CC 2018-2019
Soit E un ensemble, A, B et C trois sous-ensembles non vides de E. On notera $\overline{A}$ le complémentaire de de A dans E.
Montrer que : $A \cap B = A \cap C \Rightarrow A \cap \overline{B} = A \cap \overline{C}$.

Exercice 17 Session1 2018-2019
Soient E un ensemble et A, B et C deux sous-ensembles de E. Nous noterons $\overline{M}$ le complémentaire de M dans E pour tout sous-ensemble M de E.
Montrez que l'on a : $A \cap (\overline{B} \cup \overline{C}) = \Big((A \setminus B) \cup (A \setminus C) \Big)$.

Exercice 18 Session2 2018-2019
Soient E un ensemble et A, B, C , D des sous-ensembles de E tous non vides.
On considère les ensembles $F = (A \cap B) \times (C \cap D)$ et $G = (A \times C) \cap (B \times D)$.

1. Donnez les ensembles F et G lorsque $E = \{1, 2, 3, 4, 5\}$, $A = \{1, 2\}$, $B = \{1, 3\}$, $C = \{1, 2, 3\}$ et $D = \{1, 3, 4\}$.
2. Montrez que l'on a toujours $F \subset G$.
3. A-t-on aussi $G \subset F$?

3 Injections, surjections et bijections

Exercice 19 ★
Déterminez parmi les applications suivantes celles qui sont injectives et celles qui sont surjectives. Vous ferez une démonstration général dans le cas positif et donnerez un contre-exemple dans le cas négatif. De plus, lorsque l'application est bijective, vous donnerez l'application réciproque.

$$\begin{array}{rccc} f: & \mathbb{Z}\times\mathbb{Z} & \to & \mathbb{Z} \\ & (x,y) & \mapsto & y-x \end{array} \qquad \begin{array}{rccc} g: & \mathbb{Z}\times\mathbb{Z} & \to & \mathbb{Z}\times\mathbb{Z} \\ & (x,y) & \mapsto & (x,xy) \end{array} \qquad \begin{array}{rccc} h: & \mathbb{R}\times\mathbb{R} & \to & \mathbb{R}\times\mathbb{R} \\ & (x,y) & \mapsto & (2x+y, x-y+1) \end{array}$$

Exercice 20 ★ Image et antécédents d'un ensemble
Soient E et F deux ensembles non vides, E_1 et E_2 deux sous-ensembles de E et F_1 et F_2 deux sous-ensembles de F. On considère f une application de E dans F. Montrez les résultats suivants :

1. $E_1 \subset E_2 \implies f(E_1) \subset f(E_2)$.
2. $f(E_1 \cup E_2) = f(E_1) \cup f(E_2)$.
3. $f(E_1) \setminus f(E_2) \subset f(E_1 \setminus E_2)$.
4. Que peut-on dire de $f(E_1 \cap E_2)$ et $f(E_1) \cap f(E_2)$?
   Trouvez un contre-exemple à $f(E_1 \setminus E_2) \subset f(E_1) \setminus f(E_2)$.
5. $F_1 \subset F_2 \implies f^{-1}(F_1) \subset f^{-1}(F_2)$.
6. $f^{-1}(F_1 \cap F_2) = f^{-1}(F_1) \cap f^{-1}(F_2)$.
7. $f^{-1}(F_1 \cup F_2) = f^{-1}(F_1) \cup f^{-1}(F_2)$.

Exercice 21 CC 2018-2019
Soit f une application d'un ensemble A dans un B.

1. Quand dit-on que f est une application injective ? surjective ? bijective ?
2. On définit l'application f par :

$$\begin{array}{rccc} f & : & \mathbb{R}\times\mathbb{R} & \to & \mathbb{R}\times\mathbb{R} \\ & & (x,y) & \mapsto & (xy,\, x^2y^2) \end{array}$$

   Montrer que f n'est pas injective. Est-elle surjective ? Est-elle bijective ?
3. On considère la fonction f de $\mathbb{R}\times\mathbb{R}$ vers $\mathbb{R}\times\mathbb{R}$ définie par

$$f(x,y) = (x-y, x+y).$$

   (a) Montrez que f est une bijection. Vous donnerez la fonction réciproque f^{-1}.

   (b) Si maintenant f est définie de $\mathbb{Z}\times\mathbb{Z}$ vers $\mathbb{Z}\times\mathbb{Z}$, montrez que f n'est plus une bijection.
4. On considère les fonctions f , g et h de $\mathbb{R}^2$ vers $\mathbb{R}^2$ définies par :

$$\begin{array}{rcl} f(x,y) & = & (x-y, xy) \\ g(x,y) & = & (x,0) \\ h(x,y) & = & (2x+y, x-y) \end{array}$$

   (a) Est-ce que f et g sont injectives ? surjectives ?

   (b) Montrer que h est une fonction bijective de $\mathbb{R}^2$ dans $\mathbb{R}^2$. Déterminer son application réciproque h^{-1}.

4 Relations binaires

Exercice 22 ★
Soit $E = \{1,2,3\}$, on définit sur E la relation $\Re = \{(1,1)(2,3)(3,2)\}$.
Quelles sont les propriétés que vérifie $\Re$?

Exercice 23 ★
Dans une université, un ensemble d'étudiants E peut choisir des activité sportives et chacun doit choisir au moins une activité. dans un ensemble de sports S. On considère les relations sur E R_1 et R_2 suivantes :

$$aR_1b \iff a \text{ et } b \text{ pratiquent au moins un sport en commun.}$$

$$aR_2b \iff a \text{ et } b \text{ pratiquent exactement les mêmes sports.}$$

1. Rappelez les définitions des propriétés suivantes : relation réflexive, relation symétrique, relation transitive, relation d'équivalence.
2. Vérifiez si R_1 est réflexive ? symétrique ? transitive ?
3. Même question pour R_2.
4. Déduisez des questions précédentes si R_1 et R_2 sont des relations d'équivalence.

Exercice 24 ★ Ordres larges et stricts
1. Quand dit-on qu'une relation binaire est une relation d'ordre large ? d'ordre strict ?
   Redonnez la définition d'un ordre partiel. Quelle propriété doit être vérifiée pour que l'ordre partiel soit un ordre total.
2. Soit $E = \{a,b,c,d\}$. On définit sur E la relation R par
   $R = \{(a,b),(c,a),(b,d),(c,d),(c,b),(a,d)\}$.
   Cette relation est-elle un ordre partiel ? Si oui l'ordre est-il large ou strict ? L'ordre est-il total ?

Exercice 25 ★ Modulo et classes d'équivalences
Soit n un entier non nul. On définit sur $\mathbb{Z}$ la relation $\Re$ par

$$a \Re b \text{ lorsque } a - b = 0 \mod n.$$

1. Montrez qu'il s'agit d'une relation d'équivalence.
2. Dans le cas où $n = 2$, quelles sont les classes d'équivalence ?
3. Dans le cas où $n = 5$,
   (a) Combien y-a-t-il de classes d'équivalences ?
   (b) Déterminez $[p]$.
   (c) Définissez une addition entre $[p]$ et $[q]$.

Exercice 26 ★ Égalité sur $\mathbb{Q}$
On définit la relation $\mathcal{R}$ sur $\mathbb{Z} \times \mathbb{Z}^*$ par

$$(a_1, b_1)\mathcal{R}(a_2, b_2) \text{ lorsque } a_1 b_2 = a_2 b_1.$$

1. Montrez que $\mathcal{R}$ est une relation d'équivalence.
2. Utilisez $\mathcal{R}$ pour définir l'égalité sur $\mathbb{Q}$.

Exercice 27 ★ Complexité des algorithmes
Soit $\mathcal{F}$ l'ensemble des applications de $\mathbb{N}$ vers $\mathbb{N}$.

1. On définit la relation binaire R sur $\mathcal{F}$ par fRg (noté $f = O(g)$)lorsque

   $$\exists k \in \mathbb{N}\ \exists N \in \mathbb{N}\ \forall n \geq N \quad f(n) \leq k\ g(n).$$

   Quelles sont les propriétés vérifiées par R ? En déduire que R n'est pas une relation d'équivalence.
2. On définit la relation binaire S sur $\mathcal{F}$ par fSg (noté $f = \Theta(g)$) lorsque

   $$\exists k_1 \in \mathbb{N}\ \exists k_2 \in \mathbb{N}\ \exists N \in \mathbb{N}\ \forall n \geq N \quad k_1 g(n) \leq f(n) \leq k_2\ g(n).$$

   Montrez que S est une relation d'équivalence.

Exercice 28 Session1 2018-2019
On définit la relation $\mathcal{R}$ sur $\mathbb{Z}^2$ par

$$(a_1, b_1)\mathcal{R}(a_2, b_2) \text{ lorsque } a_1 + b_2 = a_2 + b_1.$$

1. Montrez que $\mathcal{R}$ est une relation d'équivalence.
2. Redonnez la définition de la classe d'équivalence $[(a, b)]$ de (a, b).
3. Déterminez $[(0, 0)]$, $[(3, 1)]$ et $[(2, 4)]$.

Exercice 29 Session1 2018-2019
Soit E un ensemble, x un élément fixé de E. On définit la relation $\mathfrak{R}$ sur l'ensemble des parties de E par : $A\ \mathfrak{R}\ B$ si et seulement si $x \in A \cup \overline{B}$ (où $\overline{B}$ désigne le complémentaire de B dans E).
Quelles sont les propriétés de cette relation ?

Exercice 30 ★ Session1 2018-2019
Dans $\mathbb{N}$, on définit une relation $<<$ par : $x << y$ s'il existe $m \in \mathbb{N}$ tel que $y = mx$.
Montrez que $<<$ est une relation d'ordre partiel large sur $\mathbb{N}$. Montrez que l'ordre n'est pas total.

Exercice 31 Session2 2018-2019
Soit E = $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. On définit sur l'ensemble produit $E \times E$ la relation R par : $(p, q)R(p', q')$ si et seulement si $p - p$' et $q - q'$ sont pairs.

1. Combien y-a-t-il d'éléments dans $E \times E$?
2. Montrez que R est une relation d'équivalence.
3. On désigne par $[(p, q)]$ la classe d'équivalence de (p, q). Déterminez les ensembles F et G tels que $[(1, 2)] = F \times G$.

Exercice 32 Session2 2018-2019

1. Quand dit-on qu'une relation est une relation d'ordre large ? d'ordre strict ? On rappellera les définitions utilisées.
2. Soit $X = \{a, b, c, d\}$. On définit sur X la relation $R = \{(a, b), (c, a), (b, d), (c, d), (c, b), (a, d)\}$. Montrer que R est une relation d'ordre partiel. Si oui l'ordre est-il large ou strict ? Est-ce un ordre total ?

Exercice 33 Graphes non orientés et relations binaires
Un graphe non orienté G est formé d'un ensemble de sommets V et d'un ensemble d'arêtes E. Une arête est constituée d'une paire de sommets $\{a, b\}$ de V, avec $a \neq b$.

1. Montrez que E est une relation binaire irréflexive et symétrique.
2. Calculez le nombre de graphes $G_n = (V_n, E)$, où $V_n = \{1, \ldots, n\}$.
3. On souhaite stocker les arêtes d'un graphe dans une liste. Donnez une relation d'ordre entre les paires de sommets pour pouvoir les placer par ordre strictement croissant.
   Remarque : la liste des arêtes est rarement utilisée comme structure de donnée d'un graphe car elle n'est pas très pratique. On lui préfère généralement la matrice d'adjacence ou le tableau de listes des voisins.

Exercice 34 ★ Treillis sur les mots binaires (n-cube)
Soit $n \in \mathbb{N}$, on définit E_n l'ensemble des mots binaires de longueur n. On munit E_n de deux lois internes $\vee$ et $\wedge$ définies de la manière suivante. Soit $a = a_1 \ldots a_n$ et $b = b_1 \ldots b_n$.

i) borne inférieure : $a \wedge b = c = c_1 \ldots c_n$, où $c_i = min(a_i, b_i)$, pour tout $i \in \{1, \ldots, n\}$.

ii) borne supérieure : $a \vee b = c = c_1 \ldots c_n$, où $c_i = max(a_i, b_i)$, pour tout $i \in \{1, \ldots, n\}$.

On écrit $a \leq b$ lorsque $a_i \leq b_i$, pour tout $i \in \{1, \ldots, n\}$ et $a < b$ lorsque $a \leq b$ et $a \neq b$.

1. Dessinez le treillis avec $n = 3$.
2. Montrez que l'on a l'équivalence $a \leq b \iff a \vee b = b$.
3. Montrez que $\leq$ est un ordre partiel large. Donnez avec le cas précédent des éléments incomparables, en déduire que l'ordre n'est pas total.
4. Montrez que E_n possède un plus petit et un plus grand élément.
5. On appelle chemin dans E_n des éléments $a^1, a^2, \ldots, a^k$ de E_n tels que $a^1 < a^2 \ldots < a^k$, la longueur du chemin est alors $k - 1$. Donnez un plus long chemin pour $n = 3$. Généralisez par n quelconque.
6. Montrez que l'on peut coder une fonction booléenne à n variables f avec un n-cube. Vous illustrerez ce codage dans le cas $n = 3$.
7. f est une fonction monotone croissante lorsque

$$a \leq b \implies f(a) \leq f(b).$$

   Donnez des exemples de fonctions monotones à 3 variables à partir du 3-cube.

Exercice 35 ★ Raisonnement sur le temps en intelligence artificielle
L'un des raisonnements les plus naturels concerne le temps. En intelligence artificielle, les tâches, les activités de la vie de tous les jours sont représentées par des intervalles. Ainsi exprimer « avant l'examen, j'ai révisé »se modélise par « R est avant E »avec R l'intervalle de temps de révision, E celui de l'examen et « est avant »une relation entre intervalles.

Dans cet exercice, nous utilisons la notation suivante : si I est un intervalle de temps, nous noterons d_I le début de I et f_I la fin de I, c'est-à-dire $I = [d_I, f_I]$. Nous considérerons les trois relations suivantes sur les intervalles de temps :

1. « A est avant B »
$$A \ \Re_1 \ B \text{ lorsque } f_A \leq d_B.$$
2. Relation « A est durant B »
$$A \ \Re_2 \ B \text{ lorsque } d_B < d_A \text{ et } f_A < f_B.$$
3. Relation « A commence au même moment que B »
$$A \ \Re_3 \ B \text{ lorsque } d_A = d_B \text{ et } f_A \neq f_B.$$

1. Pour ces trois relations binaires, quelles sont les propriétés vérifiées parmi les suivantes : réflexivité, irréflexivité, symétrie, antisymétrie, transitivité ?
2. En déduire lesquelles sont des relations d'équivalence et des relations d'ordre (en précisant le cas échéant si l'ordre large ou strict et si l'ordre est total).
3. Montrez que l'on a
$$(A \ \Re_1 B \wedge C \ \Re_2 \ B) \implies A \ \Re_1 C.$$

5 Combinatoire

5.1 Choix successifs

Exercice 36 ★ Principe des choix successifs
Dans un restaurant au menu figurent 4 entrées (carottes rapées, oeufs durs mayonnaise, salade, charcuterie), 3 plats (rôti de bœuf, poisson, filet de dinde), 3 accompagnements (épinards, riz, frites) et 4 desserts(fromage, yaourt, pomme, crème caramel).

1. Combien de menus peut-on composer ?
2. Pour des raisons diététiques, on interdit certaines combinaisons : combien de menus sans frites ni charcuterie peut-on composer ?
3. Combien de menus peut-on composer sans avoir à la fois les œufs dans les oeufs mayonnaise et dans la crème caramel (on peut prendre l'un des deux mais pas les deux) ?

Exercice 37 ★ Principe des choix successifs
Utilisez le principe des choix successifs pour calculer

1. le nombre d'éléments de $\mathcal{P}(E)$ pour un ensemble E de cardinal n.
2. le nombre de mots de longueur n sur l'alphabet $\mathcal{A} = \{a, b, c\}$.
3. le nombre de fonctions booléennes à n variables.

Exercice 38 ★ Mains au poker
Une main au poker est constituée d'un ensemble de cinq cartes. On considère ici que les cartes sont prises dans un jeu de 32 cartes.

1. Calculez le nombre de mains possibles.
2. Calculez le nombre de mains avec cinq hauteurs différentes.
3. Calculez le nombre de mains constituées d'une seule paire (deux cartes de la même hauteur et trois autres hauteurs).
4. Calculez le nombre de mains constituées de deux paires et d'une cinquième carte d'une troisième hauteur.
5. Calculez le nombre de brelan (trois cartes de la même hauteur et 2 autres hauteur).
6. Calculez le nombre de full (un brelan et une paire).
7. Calculez le nombre de carré (quatre cartes de la même hauteur)
8. Faire la somme des six derniers résultats obtenus. Que remarquez vous ?

5.2 Coefficients binomiaux

Exercice 39 ★ **Combinaisons et coefficient binomiaux**
On considère une collection de 10 timbres tous différents. On veut constituer une pochette avec 5 de ces 10 timbres.

1. Calculer K le nombre de façons possibles de constituer une telle pochette.
2. On suppose que la collection comprend 5 timbres noirs, 2 timbres rouges et 3 timbres verts.
   (a) Parmi les K pochettes possibles, combien se compose de 3 timbres noirs et 2 timbres verts ?
   (b) Parmi les K pochettes possibles, combien se compose de 3 timbres d'une même couleur et 2 timbres d'une autre couleur mais semblable.

Exercice 40 ★ **Formule du triangle de Pascal**

$$\binom{n}{p-1} + \binom{n}{p} = \binom{n+1}{p}. \tag{1}$$

1. Montrer directement l'équation (1) en écrivant le nombre de combinaisons en fonction de factorielles.
2. On considère les deux ensembles $E_{n+1} = \{e_1, \ldots, e_{n+1}\}$ et $E_n = \{e_1, \ldots, e_n\}$. Soit $p \leq n$, combien existe-t-il de parties A de E_{n+1} de cardinal p tel que e_{n+1} appartienne à A (respectivement e_{n+1} n'appartienne pas A) ? En déduire l'équation (1).

Exercice 41 ★ **Coefficient binomial et binôme de newton**

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k \, y^{n-k}. \tag{2}$$

1. Réécrivez l'équation (2) pour $x = y = 1$.
2. Retrouvez le nombre de parties d'un ensemble fini.

Exercice 42 Soit A et B deux ensembles disjoints de cardinaux respectifs a et b. Soit E l'ensemble des parties de $A \cup B$ qui ont n éléments.

1. En déterminant le cardinal de E montrer que l'on a

$$\binom{a+b}{n} = \sum_{k=0}^{n} \binom{a}{k} \binom{b}{n-k}.$$

2. En déduire que $\binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{k}^2$

Exercice 43 Coefficient multinomial

$$(x_1 + \ldots + x_m)^n = \sum_{\substack{(a_1,\ldots,a_m) \\ a_1+\ldots+a_m=n}} \binom{n}{a_1, \ldots, a_m} x_1^{a_1} \ldots x_m^{a_m}, \tag{3}$$

$$\text{où } \binom{n}{a_1, \ldots, a_m} = C_n^{a_1,\ldots,a_m} = \frac{n!}{a_1! \ldots a_m!}.$$

Nous allons voir comment utiliser ces coefficients multinomiaux pour dénombrer les anagrammes d'un mot. Un anagramme d'un mot est obtenu en permutant les lettres de ce mot. Dans cet exercice, on ne se préoccupe pas de savoir si ces anagrammes ont un sens.

1. Donnez le nombre d'anagrammes des mots *fourmis*, *premier* et *clémentine*.
2. Généralisation : on dispose de n lettres non toutes distinctes :
   q_1 lettres a_1, ...,q_p lettres a_p telles que $q_1 + q_2 + \ldots + q_p = n$.
   Combien de mots de longueur n peut-on former avec ces n lettres ?

Exercice 44 ★ Anagrammes et coefficients multinomiaux
On veut compter des anagrammes de mots c'est à dire des mots qui sont écrits exactement avec les mêmes lettres (on ne demande pas que le mot ait un sens ou existe dans un dictionnaire).

1. Le mot RELATION contient 4 consonnes (L,R,T,N) et 4 voyelles (0,I,A,E).
   (a) Combien y-a-t-il d'anagrammes du mot RELATION ?
   (b) Combien y-en-a-t-il qui sont formées de consonnes et voyelles en alternance (comme RELATINO) ?
   (c) Combien y-en-a-t-il qui ne comporte pas les lettres N et T à la suite (dans n'importe quel ordre)
   (d) Combien y-a-t-il d'anagrammes tels que les 4 voyelles (c'est à dire les lettres E, A, I, O) soient les unes à côté des autres ?
2. Combien y-a-t-il d'anagrammes du mot EQUIVALENCE ?
   Combien y en a-t-il où les lettres identiques sont côte à côte ?

Exercice 45 ★ Partitions d'entier
Soient n et $r \in \mathbb{N}^*$. On cherche $x_1, \ldots, x_r$, r éléments de $\mathbb{N}$, vérifiant l'équation :

$$x_1 + \ldots + x_r = n. \tag{4}$$

1. Réécrire l'équation en représentant les x_i en base unaire.
   En déduire le nombre de solutions de (4).
2. On suppose maintenant que les x_i ne peuvent pas être nuls.
   Comment se ramener au problème précédent ?

5.3 Divers

Exercice 46 ★ Principe des tiroirs
Un magicien demande à une personne de l'auditoire de choisir douze nombres entre 1 et 99. Il affirme alors être sûr que deux d'entre-eux ont choisi des nombres tels que leur différence donne un nombre formé de deux chiffres identiques. Quel est son truc ?

Exercice 47
Des parents veulent offrir à leur enfant des bandes dessinées pour son anniversaire parmi les nouveautés. Celles-ci sont rangées par catégories :

— humour – 5 nouveautés

— manga – 6 nouveautés

— comics – 3 nouveautés

— science fiction – 2 nouveautés

— aventure – 4 nouveautés

Donnez le nombre de possibilités pour chacun des cas suivants :

1. Supposons que ces parents peuvent acheter autant de livres qu'ils le souhaitent, mais au moins 1 (ils peuvent acheter un livre, ou deux livres, ou trois livres ...).
   Combien de possibilités ont-ils ?
2. S'ils achètent un livre par catégorie combien ont-ils de possibilités ?
3. Ils décident d'acheter exactement deux livres.
   Combien y-a-t-il de possibilités d'avoir les deux livres dans la même catégorie ?
4. Combien de livres doivent-ils acheter au minimum pour être sûr d'avoir au moins deux livres d'une même catégorie ?

Exercice 48 ★ Déplacements sur un échiquier
On suppose que le roi blanc est placé sur la case $a1$ et le roi noir sur la case $h8$ (voir la figure ci-dessous) et que les deux rois ne se déplacent que d'une case, soit vers le haut, soit à droite.

8	∗							
7		∗						
6			∗					
5	•			∗				
4					∗			
3						∗		
2							∗	
1	∘							∗
	a	b	c	d	e	f	g	h

1. Le roi blanc veut aller jusqu'à la case $h8$. Combien de chemins peut-il emprunter ?
2. Pour chacun des points de la diagonale tracée sur la figure, donnez le nombre de chemins que le roi blanc peut parcourir en passant par ce point.
3. Déduisez des deux questions précédentes l'égalité

$$\binom{14}{7} = \sum_{i=0}^{7} \binom{7}{i}^2.$$

4. Le roi noir veut également aller jusqu'à la case $h8$. Combien de chemins peut-il emprunter ?

Exercice 49 Nombre de relations binaires
Soit E un ensemble à n éléments avec $n \geq 2$.
On s'intéresse au nombre de relations binaires sur E.

1. Combien y a-t-il de relations binaires sur E ?
2. Combien y a-t-il de relations binaires réflexives sur E ?
3. Combien y a-t-il de relations binaires irréflexives sur E ?
4. Combien y a-t-il de relations binaires symétriques sur E ?
5. Combien y a-t-il de relations binaires antisymétriques sur E ?

5.4 Sécurité des mots de passe

Bien que plusieurs bases de mots de passe ont été piratées, l'utilisation d'un mot de passe reste une des méthodes les plus courantes pour s'authentifier pour accéder à un site ou un service. Le principal inconvénient est que la plupart des utilisateurs choisissent un mot de passe trop facile à trouver. La combinatoire permet de calculer l'espace de recherche qui doit être suffisamment grand.

Exercice 50 Codes d'un cadenas
Le code d'un cadenas est composé de 6 chiffres tous pris entre 0 et 9.

1. Combien y a t-il de codes différents possibles ?
2. Combien y-a-t-il de codes comportant des chiffres tous différents ?
3. Combien de codes comportent au moins 2 chiffres 0 ?
4. Combien de codes comportent au plus 4 chiffres 1 ?
5. Combien de codes sont fabriqués avec exactement 2 chiffres différents (mais sont toujours à 6 chiffres) ?
6. Combien de codes sont des palindromes (c'est à dire se lisent de la même façon de gauche à droite et de droite à gauche comme 123321) ?

Exercice 51 ★ Recherche d'un mot de passe dans un ensemble de mots

1. Soit $E = \{M_1, \ldots, M_n\}$ un ensemble contenant n mots. On dispose d'un mot $M \in E$. On souhaite énumérer tous les mots de E jusqu'à trouver M : on énumère M_1, puis M_2 ... On suppose que nous avons la même probabilité d'avoir $M = M_1, M = M_2, \ldots, M = M_n$. Montrez qu'il faut en moyenne énumérer $\frac{n+1}{2}$ mots avant de trouver M. On appellera coût moyen de la recherche de M dans E ce nombre. Obtient-on le même résultat si l'on change d'ordre d'énumération ?

   Remarque : si les mots de E sont triés, il est possible de retrouver M avec un coût de $\log_2 n$ (recherche dichotomique). Mais dans les applications, nous n'avons pas la valeur de M, seulement la valeur $h(M)$ où h est une fonction de hachage pour laquelle il est difficile de retrouver M à partir de $h(M)$. Dans ce cas, le fait de trier les hachés (les valeurs $h(M)$) n'aide pas la recherche.
2. Soit $\mathcal{A}$ un alphabet contenant m lettres. Notons $\mathcal{A}^l$ l'ensemble des mots sur $\mathcal{A}$ de longueur l. Donnez le coût moyen de recherche lorsque $E = \mathcal{A}^l$.
3. Quelle longueur de l faut-il pour avoir un coût supérieur à 10^{10} pour l'alphabet $\mathcal{D} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$? Même question pour alphabet $\mathcal{L} = \{a, \ldots, z\}$.
   Y-a-t-il plus de mots sur $\mathcal{D}$ de longueur 11 que de mots sur $\mathcal{L}$ de longueur 7 ?

5.5 Annales

Attention : vous devez justifier toutes les réponses pas uniquement donner des formules. Il n'est pas demandé de faire les applications numériques.

Exercice 52 CC 2018-2019

1. Combien d'anagrammes peut-on faire à partir du mot HALLOWEEN ?
2. Combien de ces anagrammes contiennent le sous-mot WEEN ?
3. Combien de ces anagrammes ne contiennent ni LL ni EE comme sous-mots ?

Exercice 53 CC 2018-2019
Un commerçant prépare des sachets de bonbons pour Halloween. Il dispose de bonbons de 4 couleurs (orange, noir, gris et blanc) et de 8 formes (araignée, fantôme, chat, chaudron, balai, sorcière, chauve-souris , chapeau).
Il décide de faire des sachets de 5 bonbons.

1. Combien y a-t-il de sachets différents ?
2. Combien y-a-t-il de sachets contenant au plus deux fantômes ?
3. Combien y a-t-il de sachets avec 2 bonbons d'une couleur et 3 bonbons de même couleur (mais d'une autre couleur) ?
4. Combien y-a-t-il de sachets avec au moins un bonbon orange et au moins un fantôme ?

Exercice 54 Session1 2018-2019
On considère la chaîne de caractères "MERRY CHRISTMAS" (15 caractères dont un caractère espace).

1. Combien y a -t-il d'anagrammes différents de cette chaîne ?
2. On ne veut pas des anagrammes qui commencent ou finissent par un espace. Combien reste-t-il d'anagrammes différents ?
3. Combien y a-t-il d'anagrammes différents qui ne contiennent ni RRR ni SS ?

Exercice 55 Session1 2018-2019
Un site internet veut générer automatiquement des mots de passe quand les gens créent un compte. Ces mots de passe doivent comporter 8 caractères pris parmi les 26 minuscules de l'alphabet et les 10 chiffres de 0 à 9. Avant de choisir et paramétrer le générateur, un responsable se pose des questions sur le nombre de mots de passe différents selon les contraintes imposées.

1. Combien y a t-il de mots de passe différents possibles ?
   Combien ne commencent pas par le chiffre 0 ?
   Combien ne contiennent pas de 0 ?
2. Combien y-a-t-il de mots comportant des caractères tous différents ?
3. Combien de mots comportent exactement 1 caractère chiffre ? au plus 2 caractères chiffres ?

Exercice 56 Session2 2018-2019
Un site internet veut générer automatiquement un mot de passe lorsqu'une personne crée un compte. Ces mots de passe doivent comporter 10 caractères pris parmi les 26 minuscules de l'alphabet, les 10 chiffres de 0 à 9 et les quatre symboles $\$, @, +$ et $*$.
Avant de choisir et de paramétrer le générateur, un responsable se pose des questions sur le nombre de mots de passe différents que l'on obtiendra selon les contraintes imposées au générateur.
Vous devez impérativement expliquer comment vous obtenez chacun des résultats pour chacune des questions suivantes.

1. Combien de possibilités a-t-on pour chaque caractère du mot de passe ?
   En déduire le nombre de mots de passe possibles.
2. Combien de mots de passe qui ne contiennent pas de symbole ?
3. Combien y-a-t-il de mots comportant des caractères tous différents ?
4. Combien de mots comportent au moins un caractère égal à @ ?
5. Combien de mots ont au plus 2 caractères qui sont des chiffres ? Détaillez les étapes nécessaires pour répondre à cette question.
6. Le générateur a sélectionné les caractères suivants : @@@*ooabcde*.
   Combien de mots de passe peut-on former avec ces 10 caractères ?
   En utilisant le principe d'inclusion-exclusion, calculez le nombre de mots de passe ne comportant ni le bloc @@@ ni le bloc *oo*.

5.6 Approfondissement

Exercice 57 ★ Paradoxe sur le nombre de combinaisons
Martin doit poser un cadenas à 8 chiffres pour fermer son casier au lycée. Malheureusement il ne possède pas de cadenas à 8 chiffres. Il décide de remplacer un tel cadenas par deux cadenas à 4 chiffres.

1. Combien y-a-t-il de combinaisons pour un cadenas à 8 chiffres.
2. Soient A et B deux ensembles de cardinalité respective n_A et n_B. Rappelez comment construire des éléments du produit cartésien $A \times B$ et donnez le cardinal de $A \times B$.
   En déduire le nombre de combinaisons des deux cadenas à 4 chiffres.
   D'après-vous Martin a-t-il fait un bon choix ?
3. Combien de combinaisons faut-il essayer en moyenne pour trouver la bonne combinaison pour le cadenas à 8 chiffres ?
4. Combien de combinaisons faut-il essayer en moyenne pour trouver la bonne combinaison des deux cadenas à 4 chiffres ?
5. Conclure.

Exercice 58 ★ Construction d'un mot suivant des règles
Certains serveurs imposent des règles pour accepter un mot de passe. Nous allons voir ici si ces règles sont très utiles.

On considère les trois alphabets $\mathcal{D} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ (chiffres), $\mathcal{L} = \{a, \ldots, z\}$ (lettres) et $\mathcal{S} = \{*, \$, \%, \#, @\}$ (caractères spéciaux).

1. L'utilisateur commence par un mot sur $\mathcal{L}$ de longueur 8. Combien a-t-il de mots possibles ?
2. Le serveur précise qu'il faut au moins un chiffre et au moins un caractère spécial. Combien y-a-t-il de mots de longueur 8 possibles ?
   Vous utiliserez le principe d'inclusion-exclusion pour trouver ce nombre.
   Est-ce que les règles augmentent beaucoup la sécurité par rapport à un mot de passe ne contenant que des lettres ?
3. Généralement les règles sont appliquées en effectuant le minimum de changement.
   L'utilisateur décide de mettre exactement un caractère spécial et un chiffre.
   Calculez le nombre de mots possibles ?
   Les utilisateurs sont encore plus prévisibles et on peut savoir avec une bonne probabilité où ils vont placer le caractère spécial et le chiffre.

4. Faites le même calcul en supposant que le caractère spécial est en avant dernière position et le chiffre en dernière position.
   En déduire que les règles ne sont pas aussi efficaces que prévu.

En conclusion, il faut différencier l'espace de recherche théorique et l'espace de recherche empirique (apprentissage sur une base de mots de passe).

6 Probabilités discrètes

6.1 Exercices de base

Exercice 59 ★ On lance trois fois une pièce de monnaie.

1. Donnez l'espace de probabilité.
2. Donnez tous les évènements possibles.
3. Donnez la distribution de probabilité dans le cas de la distribution uniforme ?
4. Donnez tous les évènements de probabilité 1/2 dans le cas de la distribution uniforme.
5. Donnez deux évènements incompatibles.
6. Donnez deux évènements indépendants.

Exercice 60 ★ On jette un dé parfaitement équilibré.

— Si on obtient un 6, on gagne 5 Euro
— Si on obtient un 5 ou un 4, on gagne 1 Euro
— Si on obtient un 3 ou un 2, on gagne 0 Euro
— Si on obtient un 1, on perd $0,5$ Euro

1. Donnez l'espace probabilisé (espace de probabilité et distribution de probabilité).
2. Calculez l'espérance de G, la variable aléatoire donnant le gain.
3. Calculez la variance et l'écart type de G.

Exercice 61
On jette un dé parfaitement équilibré. Si on obtient un 6, on gagne 5 Euros, si on obtient un 5 ou un 4, on gagne 1 Euro, si on obtient un 3 ou un 2, on gagne 0 Euro, si on obtient un 1, on perd 0.5 Euro.
Soit X la variable aléatoire correspondant au gain dans ce jeu.
Calculer l'espérance mathématique, la variance et l'écart type de X.

Exercice 62 On lance trois fois une pièce truquée pour laquelle la probabilité d'obtenir face vaut $\frac{2}{3}$.

1. Donnez l'espace probabilisé.
2. On définit une variable aléatoire X en associant à chaque tirage le plus grand nombre de faces successifs obtenus. Déterminer cette variable aléatoire ainsi que sa distribution.
3. Calculez l'espérance de X.
4. Calculez la variance de X.

Exercice 63 ★ Jeu équitable
Dans un jeu de hasard, l'espérance mathématique E du jeu correspond gain qu'un joueur peut espérer retirer du jeu. On dit que le jeu est favorable au joueur si E est positif, défavorable si E est négatif et équitable lorsque $E = 0$.
Un joueur lance deux pièces de monnaie bien équilibrées.

1. Donnez l'espace probabilisé.
2. Le joueur gagne 5 euros s'il obtient 2 faces, 2 euros s'il obtient une face et 1 euro s'il n'obtient aucune face. Déterminez la variable aléatoire associée au gain. Combien doit-il payer pour jouer pour que le jeu soit équitable ?
3. Même question lorsque chacune des deux pièces a deux chances sur trois de tomber sur face.

Exercice 64 Jeu équitable
Un joueur lance un dé non pipé.

1. Donnez l'espace probabilisé.
2. Si le dé tombe sur un nombre premier, il gagne en euros la somme égale à ce nombre. Si le dé tombe sur un nombre qui n'est pas premier, il perd ce même nombre toujours en euros. Est-un jeu équitable ?

Exercice 65 Évènements indépendants
On lance trois fois une pièce de monnaie équilibrée. On considère les évènements suivants :

— A : « Le dernier lancer vaut `Face` »
— B : « On obtient deux fois `Face` »
— C : « le deuxième lancer vaut `Face` »

1. Donnez l'espace de probabilité E et la distribution de probabilité.
2. Donnez les éléments des évènements A, B et C.
3. Vérifiez si A et B sont indépendants.
4. Vérifiez si A et C sont indépendants.

Exercice 66
On lance trois fois une pièce truquée pour laquelle $p(F) = \frac{2}{3}$.
Donnez E l'espace de probabilité. On définit une variable aléatoire sur E en associant à chaque tirage le plus grand nombre de `Face` successives. Calculez l'espérance de X.

Exercice 67 ★ Paradoxe des anniversaires
On suppose qu'il y a toujours 365 jours par an et que les naissances sont réparties uniformément sur l'année. Soit k un entier naturel, on considère un groupe de k personnes.

1. Donnez l'espace probabilisé.
2. si $k > 365$, quelle est la probabilité que deux personnes de ce groupe fêtent leur anniversaire le même jour ?
3. si $k < 365$, déterminez p_k la probabilité que deux personnes de ce groupe fêtent leur anniversaire le même jour ?
4. déterminez k_0 le plus petit k tel que $p_k \geq 1/2$. Comparez k_0 avec 365.

6.2 Somme de variables aléatoires

Exercice 68 (Essais de Bernoulli, somme de variables aléatoires)
On lance une pièce de monnaie équilibrée 10 fois. On définit une variable aléatoire élémentaire X_i pour le $i$ème lancer qui prend la valeur 1 lorsque le résultat du lancer est pile et 0 lorsque e résultat est face.

1. Donnez l'espace de probabilité pour un lancer. Calculez l'espérance et la variance.

2. Donnez l'espace de probabilité pour les 10 lancers. On définit X la variable aléatoire donnant le nombre de résultats pile. Calculez l'espérance et la variance de X. Vous justifierez vos calculs.
3. On suppose maintenant que la pièce est truquée. Nous avons 3 chances sur 5 d'obtenir un pile à chaque lancer. Donnez l'espérance et la variance avec cette nouvelle distribution de probabilité.

Exercice 69
On jette trois fois un dé à 6 faces numérotées de 1 à 6. On suppose que ce dé est équilibré.

1. Donnez l'espace probabilisé correspondant à un jet de dé.
2. Donnez E l'espace probabilisé de cette expérience aléatoire en utilisant la question 1. Montrez que la distribution de probabilité est l'équiprobabilité. Déduisez-en comment déterminer la probabilité d'un évènement.
3. On définit la variable aléatoire élémentaire X_i pour le jet i, $i \in \{1, 2, 3\}$, avec X_i qui prend la valeur 1 si le résultats est $1, 2, 3$ ou 4, qui prend la valeur 2 lorsque le résultat est 5 et qui prend 6 lorsque le résultat est 6. Calculez l'espérance et la variance de X_i.
4. On définit la variable aléatoire $X = X_1 + X_2 + X_3$. Calculez l'espérance et la variance de X. Justifiez vos calculs. pourquoi ne faut-il pas calculer directement l'espérance et la variance sans passer par les variables élémentaires X_1, X_2 et X_3 ?

6.3 Lois classiques

Exercice 70 *Loi de Bernoulli et loi binomiale* ★
On jette dix fois un dé à six faces numérotées de 1 à 6. Soit X la variable aléatoire donnant le nombre de fois où le résultat d'un lancer vaut 1 ou 6.

1. Donnez la loi de probabilité de X.
2. Soit $i \in \{0, \ldots, 10\}$. Calculez la probabilité que X vaille i.
3. Calculez l'espérance et la variance de X.

Exercice 71 *Loi de Bernoulli et loi binomiale* ★
De plus en plus d'examens sont jugés par un QCM, nous allons étudier quelques cas.
On considère un QCM de 20 questions, chaque question comportant 4 réponses proposées (différentes).

1. Pour éviter les problèmes de "copiage", les questions sont mélangées pour faire des sujets un peu différents, et à l'intérieur d'une question les réponses proposées sont elles-mêmes mélangées. Combien peut-on faire de QCM différents ?
2. On suppose que chaque question a exactement une bonne réponse et qu'un questionnaire n'est validé que si pour chaque question exactement une réponse a été donnée. Un étudiant décide de répondre complètement au hasard. Soit X la variable aléatoire correspondant au nombre de questions justes.
   (a) Quelle est la probabilité qu'il ait toutes les bonnes réponses ?
   (b) Quelle est la probabilité qui ait exactement 10 questions justes ?
   (c) Quelle est la loi de X et donc l'espérance de X ?
   (d) Quelle est la probabilité qu'il ait la moyenne ?
3. Evariste est un étudiant travailleur dont les enseignants estiment qu'il a une probabilité égale à 0,7 de répondre juste à chacune des questions. Quelle note peut-il espérer ? Quelle est la probabilité qu'il ait au moins 18 ?

4. On décide d'attribuer 1 point à chaque réponse juste et de retirer n points si la réponse est fausse. Soit Y la variable aléatoire correspondant à la note ainsi obtenue. Quelle est la note moyenne obtenue par les étudiants qui répondent au hasard ? Quelle est la note espérée par Evariste ?

Exercice 72 *Loi géométrique*
Un gardien de nuit doit ouvrir une porte dans le noir, avec n clefs dont une seule est la bonne.

1. Donner la loi de probabilité du nombre d'essais nécessaires s'il essaie les clefs une à une sans utiliser deux fois la même. Donner l'espérance et la variance.
2. Lorsque le gardien est ivre, il mélange toutes les clefs à chaque tentative. Quelle est alors la loi de X ? Donner l'espérance et la variance dans ce cas.

Exercice 73 *Loi géométrique*
On lance une pièce jusqu'à ce que l'on obtienne deux résultats successifs (pile ou face) identiques.

1. Quelle est la probabilité pour que n lancers soient nécessaires ?
2. Quelle est la probabilité pour que l'expérience s'arrête avant le 6ème jet ?
3. Soit X le nombre de lancers. Calculez l'espérance et la variance de X.

6.4 Annales

Exercice 74 Session1 2018-2019
Un joueur lance un dé à 6 faces. Si le dé tombe sur le 6 le joueur gagne 20 euros, si le dé tombe sur le 1 alors il perd 25 euros. Si le dé tombe sur une des autres faces le gain est de 5 euros.

1. On suppose que le dé est bien équilibré. Soit X la variable aléatoire correspondant au gain. Déterminer la distribution de cette variable aléatoire.
   Que vaut l'espérance de cette variable ? Le jeu est-il équilibré ? Combien faut-il miser pour qu'il le soit ?
2. En fait le dé n'est pas équilibré. La probabilité d'obtenir le 6 est 3 fois plus grande que celle d'obtenir les autres faces (qui elles ont toutes la même probabilité).
   Quelle est la probabilité d'obtenir le 6 ? le 1 ?
   Si Y est la variable aléatoire correspondant au gain dans ce cas du dé pipé, déterminer la distribution de Y et l'espérance de Y.
3. On garde ce dé pipé et on le lance 12 fois de suite. On appelle Z la variable aléatoire correspondant au nombre de fois où le 6 a été obtenu. Quelle est la probabilité que Z=12 ? que Z= 3 ?
   Quelle est la loi suivie par Z ? que vaut l'espérance de Z ?

Exercice 75 Session2 2018-2019
On souhaite proposer un jeu de paris avec une pièce de monnaie.

1. On effectue l'expérience aléatoire suivante : on jette une pièce de monnaie trois fois de suite. Donnez l'espace de probabilité.
   Combien a-t-on d'évènements possibles ?
2. On suppose avoir la distribution uniforme sur cet espace de probabilité.
   Redonnez la définition de la distribution uniforme.
   On considère E_1 l'évènement « les trois jets de la pièce ont donné la même valeur »et E_2 l'évènement « Le premier jet de la pièce donne pile et le second donne face ».
   Montrez que E_1 et E_2 ont tous les deux une probabilité $1/4$ et que E_1 et E_2 sont incompatibles.
3. Soit r le résultat de l'expérience aléatoire. On définit une variable aléatoire X qui prend la valeur 10 si r appartient à E_1, -5 si r appartient à E_2 et -1 si r n'appartient ni à E_1 ni à E_2. Calculez l'espérance de X. On suppose que X correspond au gain du jeu, est-ce que le jeu est équitable ?

7 Cryptographie

La cryptographie est l'art et la science du chiffrement. Développée au départ pour des objectifs militaires, ses applications se sont généralisées, elle est utilisée pour le chiffrement, les signatures numériques, l'authentification et beaucoup d'autres applications. La combinatoire et les probabilités interviennent de manière centrale pour quantifier certaines attaques.

Exercice 76 ★ Attaque par rencontre au milieu
En cryptographie symétrique, on utilise une même fonction pour chiffrer et déchiffrer. Soit K la clef de chiffrement et M un message. Notons $C = f_K(M)$ le message chiffré obtenu à partir de M. Nous avons alors $f_K(C) = M$.

La cryptanalyse consiste à trouver un texte en clair à partir d ?un texte chiffré sans posséder la clé de chiffrement. Une méthode utilisée pour y parvenir s'appelle une attaque.

On considère ici le chiffrement d'un message M avec deux clefs différentes K_1 et K_2.
Dans un premier temps, on obtient $C_1 = f_{K_1}(M)$ et dans un second temps on calcule $C_2 = f_{K_2}(C_1)$.

L'attaquant possède M et une valeur C_2, il cherche une paire des clefs (K_1, K_2).

On suppose ici que K_1 et K_2 sont des clefs de longueur 56 (mots binaires de longueur 56).

Comme niveau de sécurité, on souhaite que l'attaquant ne puisse pas trouver (K_1, K_2) en moins de 2^{64} essais en moyenne.

1. Combien l'attaquant doit-il tester de paires (K_1, K_2) dans le pire des cas ? A-t-on la sécurité souhaitée ?
2. Maintenant l'attaquant décide de procéder différemment. Il essaie toutes les clefs K_1 possibles et stocke pour chacune de ces clefs les valeurs $(K_1, f_{K_1}(M))$ dans une base de données. Combien doit-il stocker de valeurs $(K_1, f_{K_1}(M))$?
3. Il essaie maintenant toutes les clefs K_2 jusqu'à trouver $C_1 = f_{K_2}(C_2)$. Pour chaque K_2, il calcule $C_1 = f_{K_2}(C_2)$ et regarde si C_1 apparaît dans la base de donnée. Si c'est le cas il a trouvé une paire (K_1, K_2) qui convient. Quelle est la complexité de l'attaque si l'on néglige le temps de recherche dans la base de donnée ? A-t-on cette fois-ci la sécurité souhaitée ?

   Remarque : Cette méthode d'attaque est de type compromis temps-mémoire. Il est possible de diminuer le nombre de valeurs stockées, mais cela augmente alors le temps de recherche. Elle a souvent été utilisée pour illustrer la faiblesse d'un protocole cryptographique, par exemple, contre le double DES (deux chiffrements successifs du DES, célèbre algorithme de chiffrement symétrique). Par contre, le triple DES (trois chiffrements successifs) résiste à ce type d'attaque.

Exercice 77 ★ Fonction de hachage Une fonction de hachage est une fonction qui prend en entrée un mot binaire $m = (m_1, \ldots, m_n)$ de taille quelconque et renvoie un mot binaire de taille $c = (c_1, \ldots, c_k)$ pour k fixé.

Nous avons une collision lorsque deux mots m_1 et m_2 renvoie vers la même valeur hachée, c'est-à-dire $h(m_1) = h(m_2)$.

1. Pourquoi est-on sûr d'avoir une collision lorsque l'on plus de $n = 2^k$ messages ?
2. Combien faut-il générer de messages en moyenne pour obtenir une collision avec un message m fixé au départ ?
3. On génère des messages $m^1, m^2, \ldots$ jusqu'à avoir une collision, c'est-à-dire deux messages m^i et m^j tels que $h(m^i) = h(m^j)$. On suppose que pour chaque message m^i et chaque mot binaire $c = (c_1, \ldots, c_k)$, nous avons
   $$\Pr(h(m^i) = c) = \frac{1}{2^k}.$$
   Quelle est la probabilité d'avoir une collision au bout de l messages générés ? Nous noterons $p(l)$ cette probabilité.

4. Posons $k = 32$. Combien faut-il de messages pour avoir plus d'une chance sur deux d'avoir une collision ? Vous donnerez un algorithme pour obtenir ce résultat.

   On montre que nous avons de manière générale l'approximation

   $$l \approx \sqrt{2 \ln 2n},$$

   car nous avons

   $$1 - p(l) \approx e^{\frac{l(l-1)}{2n}}.$$

   Par exemple, pour $n = 2^{32}$, nous avons $\sqrt{2 \ln 2n} = 77162$.
   On s'aperçoit que la collision de deux valeurs quelconques est en racine carré du nombre de messages possibles, alors que la recherche d'un message fixé est de complexité linéaire par rapport au nombre de messages possibles. Elle est donc beaucoup plus facile à obtenir. En terme de mémoire, nous devons cependant stocker tous les messages générés pour pouvoir vérifier si le dernier message généré a déjà été généré.

8 Annales 2019-2020

8.1 CC octobre 2019

Exercice 78 Ensembles
Soient E un ensemble et A, B, C , D des sous-ensembles de E tous non vides.

1. Montrer que :
   $(A \times C) \cup (B \times D) \subset (A \cup B) \times (C \cup D)$?
2. Construire un contre-exemple pour montrer que l'on n'a pas toujours l'inclusion inverse $(A \cup B) \times (C \cup D) \subset (A \times C) \cup (B \times D)$

Exercice 79 Injection, surjection, bijection
Soit f une application d'un ensemble A dans un B.

1. Quand dit-on que f est une application injective ? surjective ? bijective ?
2. On définit l'application f de $\mathbb{R}^2$ vers $\mathbb{R}^2$ par $f(x, y) = (x + y^2, y^2)$
   Montrer que f n'est pas injective. Est-elle surjective ? Est-elle bijective ?
3. On considère la fonction g de $\mathbb{R}^2$ vers $\mathbb{R}^2$ définie par : $g(x, y) = (2x + y, x - 2y)$
   Montrer que g est bijective de $\mathbb{R}^2$ dans $\mathbb{R}^2$. Déterminer son application réciproque g^{-1}

Exercice 80 Induction
On rappelle le schéma d'induction pour calculer la hauteur d'un arbre binaire :

i) L'arbre vide $\emptyset$ vérifie $h(\emptyset) = -1$

ii) Soient B et C deux arbres binaires et $A = (\bullet, B, C)$.

$$h(A) = sup(h(B), h(C)) + 1.$$

On définit inductivement un poids aux arbres binaires avec le schéma d'induction suivant :

i) L'arbre vide $\emptyset$ vérifie $M(\emptyset) = 0$

ii) Soient B et C deux arbres binaires et $A = (\bullet, B, C)$ alors $M(A) = 2sup(M(B), M(C)) + 1$

Montrez par induction que tout arbre binaire A vérifie : $M(A) = 2^{h(A)+1} - 1$.

Exercice 81 Relations
On définit sur $\mathbb{R}$ la relation $\mathcal{R}$ par $x\mathcal{R}y$ lorsque $x^2 - y^2 = x - y$.

1. Montrez qu'il s'agit d'une relation d'équivalence.
2. Soit $x \in \mathbb{R}$. Déterminer sa classe d'équivalence.

Exercice 82 Combinatoire

1. Le mot JACQUES contient 4 consonnes (J,C,Q,S) et 3 voyelles (A,U,E).
   (a) Combien y-a-t-il d'anagrammes du mot JACQUES ?
   (b) Combien y-a-t-il d'anagrammes commençant et finissant par une consonne ?
   (c) Combien y-a-t-il d'anagrammes commençant et finissant par une voyelle ?
   (d) Combien y-a-t-il d'anagrammes commençant par une voyelle et finissant par une consonne ?
   (e) Combien y-a-t-il d'anagrammes ne contenant pas le mot EAU ?
2. Combien y-a-t-il d'anagrammes du mot CHIRAC ? et "JACQUES CHIRAC" ? (on comptera l'espace comme une lettre.

8.2 Examen session1 décembre 2019 – extraits

Exercice 83 Mots de passe
On considère $\mathcal{M}$ l'ensemble des mots de longueur 10 construit sur l'alphabet $\mathcal{A} = L \cup U \cup D \cup S$, où

— L est l'ensemble des 26 lettres minuscules.
— U est l'ensemble des 26 lettres majuscules.
— D est l'ensemble de chiffres $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.
— S est l'ensemble des caractères spéciaux $\{\$, \#, !, @\}$.

1. Donnez la cardinalité (nombre d'éléments) de $\mathcal{M}$.
2. On découpe un mot de $\mathcal{M}$ en blocs de lettres d'un même sous-ensemble L, U, D ou S en précisant le nombre de lettres pour chaque bloc, on appellera classe un tel découpage. Par exemple, $U_1L_7D_1S_1$ est la classe des mots de $\mathcal{M}$ commençant par une majuscule, suivi de 7 lettre minuscules, puis d'un chiffre et enfin d'un caractère spécial. Par exemple, $Motpasse0\$$ et $Azertyui1\#$ sont des mots de $U_1L_7D_1S_1$.
   Donnez le nombre de mots des classes $U_1L_7D_1S_1$, $U_1L_8D_1$, L_8S_2.
3. On sait qu'un mot appartient à la classe $U_1L_8D_1$. On génère les mots de la classe un par un. Combien de mots doit-on générer en moyenne pour retrouver ce mot ?
4. Combien de mots peut-on former avec des classes utilisant les blocs L_6, U_1, D_2 et S_1 ? Les blocs peuvent être dans n'importe quel ordre.
5. Soient n et $r \in \mathbb{N}^*$. On rappelle que le nombre de r-uplet $(x_1, \ldots, x_r)$, constitués de r d'éléments de $\mathbb{N}^*$, vérifiant l'équation : $x_1 + \ldots + x_r = n$ vaut $\binom{n-1}{r-1}$.
   Calculez le nombre de classes que l'on peut former avec un bloc de U, suivi d'un bloc de L, puis d'un bloc de D (par exemples, $U_1L_8D_1, U_2L_5D_3$).
   Calculez le nombre de classes lorsque les trois blocs de U, L et D peuvent être dans n'importe quel ordre.

Exercice 84 Ensembles
Soient A, B et C trois ensembles non vides.

1. Donner un exemple où $A \cup B = A \cup C$ et $B \neq C$.
2. Donner un exemple où $A \cap B = A \cap C$ et $B \neq C$.

3. Montrer que : $\big(A \cup B = A \cup C \quad \text{et} \quad A \cap B = A \cap C\big) \Longrightarrow B = C$.

Exercice 85

1. Soit f une application d'un ensemble E dans un ensemble F. Quand dit-on que f est une application injective ? surjective ? bijective ?
2. On considère la fonction f définie de $\mathbb{R}^3$ dans $\mathbb{R}^2$ par $f(x, y, z) = (x + z, y + z)$.
   Que peut-on dire de f ?
3. Montrer que la fonction g définie de $\mathbb{R}^2$ dans $\mathbb{R}^2$ par$g(x, y) = (2y - x, x + y)$ est une fonction bijective dont on donnera la fonction réciproque

Exercice 86
On dit qu'une relation $\Re$ sur un ensemble E est circulaire si pour tous a, b, c éléments de E :
$(a\Re b$ et $b\Re c) \implies (c\Re a)$.
Montrez qu'une relation est une relation d'équivalence si et seulement si elle est réflexive et circulaire.
Donnez un exemple de relation circulaire qui n'est pas une relation d'équivalence.

Exercice 87
Soit E un ensemble et A un sous-ensemble fixé de E non vide. On définit sur $\mathcal{P}(E)$ la relation $\Re$ par $X\Re Y$ lorsque $A \cap X \subset A \cap Y$

1. Montrer que cette relation est réflexive et transitive. On donnera la définition de ces propriétés.
2. On suppose $E = \{a, b, c, d, e\}$ et $A = \{a\}$; montrer que la relation $\Re$ n'est pas antisymétrique.
3. La relation $\Re$ est-t-elle une relation d'ordre ? (vous justifierez votre réponse).

Exercice 88 On joue avec deux dés à 5 faces prenant les valeurs $\{1, 2, 3, 4, 5\}$, un dé blanc et un dé rouge. On lance les deux dés et on suppose que les deux dés sont bien équilibrés.

1. Quel est l'univers des possibles (ou espace de probabilité) ?
   Quel est la distribution de probabilité ?
2. Le premier jeu est le suivant : on gagne la somme des deux dés s'ils sont différents, et on doit payer cette somme si on fait un double (deux dés identiques). Soit X la variable aléatoire correspondante.
   (a) Quelles sont les valeurs prises par la variable X ?
   Déterminer la distribution de cette variable aléatoire.
   (b) Que vaut l'espérance de cette variable aléatoire X. Vous donnerez la définition de l'espérance.
   Le jeu est-il équilibré ?
3. En fait les dés ne sont pas équilibrés mais ils ont le même biais : le 5 et le 1 tombent 4 fois plus que les autres faces.
   (a) Donner la distribution de probabilité pour chaque dé.
   (b) Quelle est la probabilité d'obtenir le double i pour chaque $i \in \{1, 2, 3, 4, 5\}$?
   (c) On définit un deuxième jeu en lançant 20 fois ces deux dés.
   À chaque lancer, on gagne si on fait un double (n'importe lequel) et on perd si on obtient deux dés différents. On notera Y la variable aléatoire qui compte le nombre de fois où on gagne.
      i. Quelle est la loi suivie par Y ?
      ii. Quelle est la probabilité de gagner exactement 10 fois ? (on demande une formule)
      iii. Quelle est l'espérance de Y ?

9 Annales 2020-2021

9.1 CC1 octobre 2020

Exercice 89 Arbres binaires

1. Soit A un arbre binaire ayant n noeuds et de hauteur h.
   Montrer par induction que $h \leq n-1$.
2. Un arbre binaire est dit localement complet si il est non vide et si chaque nœud a 0 ou 2 descendants.
   (a) Ecrire le schéma d induction des arbres localement complets.
   (b) Dresser la liste des arbres binaires localement complets de hauteur 2.

Exercice 90 Ensembles
Si X et Y sont des ensembles avec $X \subset Y$, on notera $\mathcal{C}_Y^X$ le complémentaire de X dans Y .
Soient E un ensemble et A et B des sous-ensembles de E tous non vides.

1. Définir $\mathcal{C}_E^A$ et $\mathcal{C}_{E\times E}^{A\times B}$
2. On considère $F = \mathcal{C}_{E\times E}^{A\times B}$ et G= $\mathcal{C}_E^A \times \mathcal{C}_E^B$. Montrer que $G \subset F$.
3. L'inclusion inverse est-elle vérifiée ? (On justifiera la réponse donnée).

Exercice 91 Injection, surjection, bijection
Soit f une application d'un ensemble A dans un ensemble B.

1. Quand dit-on que f est une application injective ? surjective ? bijective ?
2. On définit l'application f par :

$$\begin{array}{rccc} f & : & \mathbb{R}\times\mathbb{R} & \to & \mathbb{R}\times\mathbb{R} \\ & & (x,y) & \mapsto & (x^2,\, y) \end{array}$$

   Que peut-on dire de f ? Est-elle injective ? Est-elle surjective ? Est-elle bijective ?
3. On considère la fonction g de $\mathbb{R}^2$ vers $\mathbb{R}^2$ définie par :

$$g(x,y) \;=\; (x-y, x+y)$$

   Montrer que g est bijective de $\mathbb{R}^2$ dans $\mathbb{R}^2$. Déterminer son application réciproque g^{-1}

Exercice 92 relations
On définit sur $\mathbb{Z}$ la relation $\mathcal{R}$ par $a\mathcal{R}b$ si et seulement si 4 divise $a^2 - b^2$.

1. Quelles sont les propriétés que doit vérifier $\mathcal{R}$ pour être une relation d'équivalence ? (on définira chacune d'entre elles).
2. Montrez que $\mathcal{R}$ est une relation d'équivalence.

9.2 DM décembre 2020

Exercice 93 Classes pour les mots de passe
On considère des mots de passe de longueur 10 sur l'alphabet $\mathcal{A} = L \cup U \cup D$ où

— $L = \{a, \ldots, z\}$ est l'ensemble des minuscules
— $U = \{A, \ldots, Z\}$ est l'ensemble des majuscules
— $D = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ est l'ensemble des chiffres

Nous noterons $\mathcal{M}$ l'ensemble des mots de longueur 10 sur $\mathcal{A}$ et $\mathcal{N} = \{L, U, D\}^{10}$.

On définit une application $f : \mathcal{M} \to \mathcal{N}$ qui a tout mot $m = m_1 \dots m_{10}$ de $\mathcal{M}$ associe le mot $n = n_1 \dots n_{10}$ où, pour tout $i \in \{1, \dots, 10\}$,

$$\begin{array}{rcl} n_i & = & L \text{ lorsque } m_i \text{ est une minuscule} \\ & = & U \text{ lorsque } m_i \text{ est une majuscule} \\ & = & D \text{ lorsque } m_i \text{ est un chiffre} \end{array}$$

Par exemple, si $m = BON000jour$, nous avons $f(m) = UUUDDDLLLL$.

On regroupe maintenant les lettres de $\{L, U, D\}$ consécutives identiques. On écrira par la suite $f(m) = U_3D_3L_4$, qui signifie que m est formé de trois majuscules, suivi de trois chiffres, suivi de quatre minuscules.

1. Donnez les cardinalités de $\mathcal{M}$ et $\mathcal{N}$.
2. Est-ce que f est injective ? surjective ? Dans le cas où f est une bijection, donnez la fonction réciproque f^{-1}.
3. Montrez que la relation binaire R sur $\mathcal{M}$ définie par $m_1 R m_2$ lorsque $f(m_1) = f(m_2)$ est une relation d'équivalence.
   Montrez que chaque mot n de $\mathcal{N}$ forme une classe d'équivalence sur $\mathcal{M}$ où les éléments de n sont les mots m tels que $f(m) = n$.
4. Proposez trois classes n_1, n_2, n_3 de $\mathcal{N}$. Construisez un élément pour chacune de ces classes. Calculez la cardinalité des ces classes. Vous utiliserez impérativement le principe des choix successifs.
5. Construisez une bijection entre les deux classes $U_3D_3L_4$ et $L_4U_3D_3$.
6. On considère maintenant des classes n contenant au moins un L, un U et un D.
   Déterminez une classe de plus grande cardinalité.
   Déterminez une classe de plus petite cardinalité.

Exercice 94

Soit $n \in \mathbb{N}$, on note $\mathcal{A}_n$ l'ensemble des arbres binaires à n nœuds et a_n le cardinal de $\mathcal{A}_n$.

1. Donnez un schéma d'induction pour construire un élément de $\mathcal{A}_n$.
2. En déduire $a_n = \displaystyle\sum_{k=0}^{n-1} a_k \; a_{n-1-k}$.

   Remarque : on admettra que a_n est égal au nombre de Catalan $\dfrac{\binom{2\,n}{n}}{n+1}$.
3. Notons $\mathcal{B}_k$ l'ensemble des arbres binaires localement complets à k feuilles et b_k son cardinal. Montrez que l'on a $b_k = a_{k-1}$, où a_{k-1} désigne le nombre d'arbres binaires à $k-1$ noeuds.

Exercice 95

On appelle arbre de calcul un arbre binaire dont :

— les feuilles sont indexées par 0 ou 1 ;

— les nœuds internes sont indexés par + ou $\times$.

Pour ces arbres, on définit la fonction f qui à tout arbre associe un entier défini de la façon suivante :

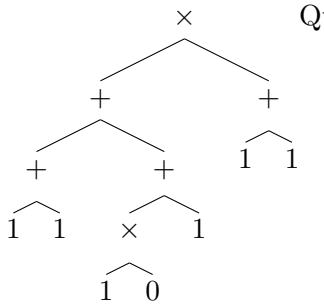
— Si l'arbre A est réduit à une feuille indexée par i, alors $f(A) = i$;

— Si la racine de l'arbre A est un nœud indexé par +, et si A a pour sous-arbres A_g et A_d alors $f(A) = f(A_g) + f(A_d)$

— Si la racine de l'arbre A est indexé par $\times$, et si A a pour sous-arbres A_g et A_d alors $f(A) = f(A_g) \times f(A_d)$

On peut remarquer qu'un arbre de calcul est localement complet.

1. Rappeler ce qu'est la hauteur d'un arbre.
2. On considère l'arbre de calcul suivant :



Quelle est la hauteur de cet arbre ?

Déterminer l'image par la fonction f définie ci-dessus de cet arbre.

3. Construire un arbre de calcul dont la valeur associée est 13. Plusieurs solutions sont bien entendu possibles, on essayera de faire un arbre pas trop volumineux....
4. Montrer par induction que pour tout arbre A, on a

$$0 \leq f(A) \leq 2^{2^{h(A)}},$$

où $h(A)$ désigne la hauteur de l'arbre A.

Exercice 96
Soient n, a, b trois entiers, E un ensemble ayant n éléments, A un sous-ensemble de E ayant a éléments, B un sous-ensemble de $E \setminus A$ ayant b éléments.

1. donnez un exemple d'ensembles E, A et B avec $n = 6$, $a = 2$ et $b = 2$.
   Donnez deux ensembles S tels que $A \subset S$.
   Donnez deux ensembles U tels que $B \subset U$ et $A \cap U = \emptyset$.
2. Combien y-a-t-il de sous-ensembles S de E tels que $A \subset S$?
3. Combien y-a-t-il de sous-ensembles U de E tels que $B \subset U$ et $A \cap U = \emptyset$?

9.3 Session2 juin 2021

Exercice 97 Combinatoire – Relations binaires
Dix sportifs d'un même club se retrouve pour préparer une compétition. Chacun possède un niveau selon les performances réalisées dans l'année. Il possède le niveau *Or* s'il a gagné une compétition, le niveau *Argent* s'il a fini deuxième à une compétition, le niveau *Bronze* s'il a fini troisième à une compétition. S'il n'a jamais fini dans les trois premières places, il a le niveau *Non classé*.

1. Soit E l'ensemble des niveaux que peuvent avoir les dix sportifs. Un élément de E attribue donc un niveau à chacun des sportifs. Donnez la cardinalité de E. Vous utiliserez soit le principe des choix successifs, soit une relation sur les produits cartésiens.
2. Soit A un sous-ensemble de E, nous noterons $\overline{A}$ le complémentaire de A dans E. Redonnez la définition de $\overline{A}$ et la cardinalité de $\overline{A}$ en fonction de celle de A et de E.
3. Soit A_1 l'ensemble des niveaux que peuvent avoir les dix sportifs lorsque aucun d'entre-eux n'a le niveau *or* et A_2 l'ensemble des niveaux que peuvent avoir les dix sportifs lorsque aucun d'entre-eux n'a le niveau *argent*. Donnez les cardinalités de A_1, A_2. Vous utiliserez soit le principe des choix successifs, soit une relation sur les produits cartésiens.
   Déduisez de la question précédente, la cardinalité de $\overline{A_1}$ et $\overline{A_2}$.

4. Calculez le cardinal de $A_1 \cap A_2$. Utilisez le principe d'inclusion-exclusion pour calculer $A_1 \cup A_2$.
5. Soit B l'ensemble des niveaux des dix sportifs tels qu'au moins un sportif a le niveau *or* et au moins un sportif a le niveau *argent*. Utilisez la réponse à la question précédente pour déterminer le cardinal de B.
   Les questions 6, 7 et 8 peuvent être traitées indépendamment des cinq premières.
6. Montrez que deux sportifs ont le même niveau.
   Quel principe utilisez-vous ?
7. Soient S_1 et S_2 deux de ces sportifs. On définit la relation binaire R par

   $$S_1 R S_2 \text{ lorsque } S_1 \text{ et } S_2 \text{ ont le même niveau.}$$

   Montrez que R est une relation d'équivalence et donnez les classes d'équivalence.
8. Soient S_1 et S_2 deux des sportifs, on définit la relation binaire $\lhd$ par $S_1 \lhd S_2$ lorsque S_1 est non classé et S_2 a une médaille ou que S_2 a une meilleure médaille que S_1. Montrez que $\lhd$ est un ordre strict. Montrez que l'ordre est partiel (c'est-à-dire qu'il n'est pas total).

Exercice 98 Combinatoire – Probabilités
On jette trois fois de suite un dé équilibré à six faces numérotées de 1 à 6.
On définit une variable aléatoire Z qui prend les valeurs suivantes :

- 10 lorsque l'on a fait 3 six
- 5 lorsque l'on a fait deux six
- 2 lorsque l'on a fait un six
- -2 lorsque l'on ne fait aucun six

1. Définissez E, l'espace de probabilité de l'expérience aléatoire.
2. Donnez la distribution de probabilité sur E.
   Soit A un évènement, donnez la probabilité de A, justifiez votre réponse.
3. On considère les évènements suivants

   $$\begin{array}{rcl} E_1 & = & \text{nous avons obtenu trois six} \\ E_2 & = & \text{nous avons obtenu deux six} \\ E_3 & = & \text{nous avons obtenu un seul six} \\ E_4 & = & \text{nous n'avons obtenu aucun six} \end{array}$$

   Calculez la cardinalité de ces quatre évènements.
   Vous devez impérativement justifier vos calculs.
4. Calculez l'espérance de Z.
5. Supposons que Z corresponde au gain d'un joueur, montrez que le jeu n'est pas équitable.
6. Nous souhaitons obtenir un jeu équitable en modifiant le gain lorsque le résultat n'a pas de six. Quelle valeur faut-il mettre ?

Exercice 99 Combinatoire
Il faut impérativement justifier les réponses. Les applications numériques ne sont pas demandées. On considère la phrase : "VIVENT LES VACANCES !" composée de 21 caractères dont 3 espaces.

1. Combien y a-t-il d'anagrammes de cette phrase ?
2. Combien y a-t-il d'anagrammes qui ne commencent pas et ne finissent pas par un espace ?
3. Combien y a-t-il d'anagrammes qui ne contiennent ni 3V successifs ni 3E successifs ?

Exercice 100 Fonctions

1. Soit f une application d'un ensemble E dans un ensemble F. Quand dit-on que f est une application injective ? surjective ? bijective ?
2. On considère la fonction f de $\mathbb{R}^3$ dans $\mathbb{R}^2$ définie par $f(x, y, z) = (x + y, x + z)$.
   Que peut-on dire de f ?
3. On considère la fonction f de $\mathbb{R}^2$ dans $\mathbb{R}^2$ définie par $f(x, y) = (x + y, xy)$.
   Que peut-on dire de f ?
4. Montrer que la fonction g de $\mathbb{R}^2$ dans $\mathbb{R}^2$ définie par $g(x, y) = (2y - x, x + y)$ est une fonction bijective dont on donnera la fonction réciproque.

Exercice 101 Arbres binaires et induction

1. Redonnez la définition d'un arbre localement complet.
2. Redonnez le shéma d'induction de $\mathcal{L}$, l'ensemble des arbres localement complets.
3. Soit $A = (\cdot, B, C)$ un arbre de $\mathcal{L}$ avec B et C différents de l'arbre vide. On note $h(A)$ la hauteur de l'arbre A.
   Redonnez la relation reliant $h(A)$, $h(B)$ et $h(C)$
   En déduire que l'on a $h(B) + h(C) \geq h(A) - 1$.
4. Montrez en utilisant le shéma d'induction sur $\mathcal{L}$ que tout arbre A de $\mathcal{L}$ vérifie la propriété $N(A) \geq 2h(A) + 1$ où $N(A)$ désigne le nombre de nœuds de l'arbre A.

Exercice 102 Ensembles et applications
Soit E un ensemble et A et B deux sous-ensembles de E. On rappelle que $\mathcal{P}(E)$ est l'ensemble des parties de E. Soit f une application définie par

$$\begin{array}{rccl} f & : & \mathcal{P}(E) & \longrightarrow & \mathcal{P}(A) \times \mathcal{P}(B) \\ & & X & \longmapsto & (X \cap A\,,\, X \cap B). \end{array}$$

1. On suppose pour cette question **uniquement** que $E = \{0, 1, 2\}$, $A = \{0, 1\}$ et $B = \{1, 2\}$.
   (a). Compléter le tableau suivant avec l'ensemble $\mathcal{P}(E)$ et les valeurs de f pour chaque élément de $\mathcal{P}(E)$

$x \in \mathcal{P}(E)$	$f(x)$
$\emptyset$	$(\emptyset, \emptyset)$
$\{0\}$	$(\{0\}, \emptyset)$
$\{0, 1, 2\}$	$(\{0, 1\}, \{1, 2\})$

   (b). Cette fonction est-elle injective ? surjective ?
2. Pour la suite de l'exercice on considère E, A et B quelconques tels que $A \subset E$ et $B \subset E$.
   (a). Donner les valeurs de $f(\emptyset)$ et de $f(\overline{A \cup B})$.
   (b). Montrer que f est injective si et seulement si $A \cup B = E$.
   (c). Le couple $(\emptyset, B)$ possède-t-il un antécédent par f ?
   (d). Montrer que f est surjective si et seulement si $A \cap B = \emptyset$.

Exercice 103 Ensembles et applications
Soit $\mathcal{B} = \{0, 1\}$ muni de l'addition et de la multiplication définies sur $\mathbb{Z}$. Soit X un ensemble quelconque et A et B deux parties de X. La fonction indicatrice de A est la fonction de X vers $\mathcal{B}$ suivante :

$$\mathbf{1}_A(x) = \begin{cases} 1 & \text{si } x \in A, \\ 0 & \text{sinon.} \end{cases}$$

1. Que peut-on dire des ensembles A et B si $\mathbf{1}_A = \mathbf{1}_B$.
2. Vérifier les expressions suivantes :

$$\begin{aligned} \mathbf{1}_{\bar{A}}(x) &= 1 - \mathbf{1}_A(x) \\ \mathbf{1}_{A\cap B}(x) &= \mathbf{1}_A(x) \cdot \mathbf{1}_B(x) \end{aligned}$$

3. On suppose que les ensembles A et B sont **disjoints**.
   Montrer que
   $$\mathbf{1}_{A\cup B}(x) = \mathbf{1}_A(x) + \mathbf{1}_B(x).$$
4. On suppose maintenant que A et B sont **quelconques**.
   Montrer que $A \cup B = A \cup (\overline{A} \cap B)$ et que A et $\overline{A} \cap B$ sont deux ensembles disjoints.
5. Déduire des questions précédentes l'expression suivante

$$\mathbf{1}_{A\cup B}(x) = \mathbf{1}_A(x) + \mathbf{1}_B(x) - \mathbf{1}_A(x) \cdot \mathbf{1}_B(x).$$

10 Annales 2021-2022

10.1 CC octobre 2021

Exercice 104 **: Induction sur les arbres binaires.**

1. Redonnez le schéma d'induction de l'ensemble des arbres binaires.
2. On définit inductivement une application qui attribue une valeur $V(A)$ à tout arbre binaire A.

   i) Si A est l'arbre vide alors $V(A) = 0$ et si A est l'arbre racine alors $V(A) = 1$.

   i) soit $A = (\cdot, A_g, A_d)$ un arbre binaire différent de l'arbre vide et de l'arbre racine.
   $V(A) = |V(A_g) - V(A_d)|$.

   Montrez par induction que tout arbre binaire A vérifie $V(A) = 0$ ou $V(A) = 1$

Exercice 105 **: Injection, surjection, bijection.**

1. Soit f une application d'un ensemble A dans un ensemble B. Quand dit-on que f est une application injective ? surjective ? bijective ?
2. On définit l'application f par

$$\begin{array}{rccc} f & : & \mathbb{R}\times\mathbb{R}\times\mathbb{R} & \to & \mathbb{R}\times\mathbb{R} \\ & & (x, y, z) & \mapsto & (x + z,\, y + z) \end{array}$$

   Montrer que f n'est pas injective. Est-elle surjective ? bijective ?

3. On définit l'application g par

$$\begin{array}{rccc} g & : & \mathbb{R}\times\mathbb{R} & \to & \mathbb{R}\times\mathbb{R} \\ & & (x,y) & \mapsto & (2y-x,\, x+y) \end{array}$$

Montrer que g est une application bijective et déterminer l'application réciproque de g.

Exercice 106 **: Relations d'ordre.**

1. Redonnez les propriétés que doit vérifier une relation R pour être une relation d'ordre partiel large.
2. Redonnez les propriétés que doit vérifier une relation R pour être une relation d'ordre partiel stricte.
   Soit E un ensemble fini de cardinalité $n \geq 2$.
   On définit sur $P(E)$ la relation binaire R par

$$A\ R\ B \text{ lorsque } A \subset B.$$

3. Montrez que R est une relation d'ordre. Précisez si l'ordre est large ou strict.
4. Montrez que l'ordre n'est pas total.

10.2 Examen session1 décembre 2021

Exercice 107 **Induction sur les arbres binaires.**

1. Redonnez la définition d'un arbre binaire localement complet.
2. Soit Alc l'ensemble des arbres binaires localement complets. Donnez le schéma d'induction de l'ensemble Alc .
3. On définit inductivement une application qui attribue une valeur $V(A)$ à tout arbre binaire A.
   i) Si A est l'arbre vide alors $V(A) = 0$ et si A est l'arbre racine alors $V(A) = -1$.
   i) soit $A = (\cdot, A_g, A_d)$ un arbre binaire différent de l'arbre vide et de l'arbre racine.
   $V(A) = V(A_g) + V(A_d) + 1$.
   (a) Donnez un arbre binaire à 5 nœuds A tel que $V(A) \neq -1$.
   (b) Montrez par induction que tout arbre localement complet A vérifie $V(A) = -1$.

Exercice 108 **Relations binaires**
Rappels sur la division euclidienne : on considère la division euclidienne d'une entier $n \in Z$ par 10. Pour tout $n \in \mathbb{Z}$, il existe deux uniques valeurs q et r tels que $n = 10q+r$ avec $q \in \mathbb{Z}$ et $r \in \{0, \ldots, 9\}$. r est appelé le quotient et r le reste.
On définit sur $\mathbb{Z}$ la relation binaire R par

$$xRy \text{ lorsque } x \text{ et } y \text{ ont le même quotient.}$$

1. Rappelez les propriétés que vérifie une relation d'équivalence.
   Redonnez à chaque fois la définition de la propriété.
2. Montrez que R est une relation d'équivalence.
3. Déterminer la classe équivalence de 150.

Exercice 109 **Probabilités**
On jette six fois un dé à cinq faces numérotées de 1 à 5.

1. Donnez E, l'espace de probabilité.
   On suppose que nous avons l'équiprobabilité. Donnez la probabilité pour chaque résultat possible de l'espace de probabilité. Donnez la probabilité d'obtenir une valeur paire. Expliquez votre calcul.
2. On définit sur E une variable aléatoire Y donnant le nombre de valeurs paires. Calculez l'espérance et la variance de Y.
3. On suppose maintenant que le dé est truqué. Il a une chance sur deux de tomber sur 1, les autres faces restent équiprobable pour ce dé.
   Calculez à nouveau l'espérance et la variance de Y.

Exercice 110 **Combinatoire et probabilités**

On suppose que les naissances sont réparties uniformément sur les jours de la semaine (du lundi au dimanche). Soit n un entier naturel et on s'intéresse au jour de semaine correspondant à la date de naissance d'une ersonne. Considérons un groupe de n personnes.

1. Donnez l'espace probabilisé et la distribution de probabilité.
2. Nous noterons p_n la probabilité que deux personnes de ce groupe soient nées le même jour de la semaine pour $n \geq 2$.
   Calculez p_n lorsque $n > 7$.
3. Calculez p_2 probabilité que deux personnes soient nées le même jour de la semaine.
4. On suppose maintenant que $n \leq 7$, calculez p_n.
5. Déterminez n_0 le plus petit entier n tel que $p_n \geq 1/2$.

Exercice 111 **Ensembles** Soit E un ensemble. Si A est un sous-ensemble de E on notera $\mathcal{C}_E^A$ le complémentaire de A dans E. Soit A et B deux sous ensembles de E.

1. Redonnez la définition de $A \Delta B$.
2. Que peut-on dire des ensembles $A \Delta A$, $A \Delta \mathcal{C}_E^A$, $A \Delta E$ et $A \Delta \emptyset$?
3. Soit A et B deux sous ensembles de E. Montrer que $A \Delta B = B$ si et seulement si $A = \emptyset$.

Exercice 112 **Anagrammes**

1. Combien y a-t-il d'anagrammes du mot PIKACHU ?
2. Combien y-a-t-il d'anagrammes du mot PIKACHU tels que les 4 consonnes (P,K,C,H) et les 3 voyelles (I,A,U) soient alternées comme dans KIPACUH ?
3. Combien y-a-t-il d'anagrammes du mot RONDOUDOU ?
4. Combien y a-t-il d'anagrammes du mot PIKACHU pour lesquels les 3 voyelles I, A et U sont les unes à côté des autres ?
5. Combien y-a-t-il d'anagrammes du mot PIKACHU dans lesquels il n'y a pas le mot PIK ni le mot CHU ?

Exercice 113 **Injection, surjection, bijection** : Soit f une application d'un ensemble A dans un ensemble B.

1. Quand dit-on que f est une application injective ? surjective ? bijective ?
2. On définit l'application f par

$$\begin{array}{rccc} f & : & \mathbb{R} \times \mathbb{R} & \to & \mathbb{R} \times \mathbb{R} \\ & & (x, y) & \mapsto & (xy,\, x - y) \end{array}$$

   Montrer que f n'est pas surjective. Est-elle injective ? bijective ?

3. On définit l'application g par

$$\begin{array}{rccc} g & : & \mathbb{R}\times\mathbb{R} & \to & \mathbb{R}\times\mathbb{R} \\ & & (x,y) & \mapsto & (x+y+1,\, 2x-y-1) \end{array}$$

Montrer que g est une application bijective et déterminer l'application réciproque de g.

10.3 Session2 juin 2022

Exercice 114 (Injections, surjections, bijections)
Soient x et $y \in \mathbb{Z}$, nous noterons x div y le quotient de la division euclidienne de x par y et x mod y son reste. On définit l'application f de $\mathbb{Z}$ vers $\mathbb{Z}\times\{0,1,2,3,4,5,6,7,8,9\}$ qui à $x \in \mathbb{Z}$ associe $f(x) = (x \text{ div } 10, x \mod 10)$.

Autrement dit, x s'écrit de manière unique $x = q*10+r$, où $q \in \mathbb{N}$ et $r \in \{0,1,2,3,4,5,6,7,8,9\}$ et $f(x) = (q,r)$.

Par exemple, si $x = 35$ alors $x = 3*10+5$ et $f(x) = (3,5)$ et si $x = 67 = 6*10+7$ alors $f(x) = (6,7)$.

1. Montrez que f est une injection.
2. Montrez que f est une surjection.
3. Montrez que f et donnez f^{-1}, son application réciproque.

Exercice 115 (Relations binaires)
Soit $\mathcal{F}$ l'ensemble des applications de $\mathbb{N}$ dans $\mathbb{N}$.
Pour tous f et g de $\mathcal{F}$, on définit sur $\mathcal{F}$ la relation binaire R par

$$f\ R\ g \text{ si et seulement si } f(x) \leq g(x) \text{ pour tout } x \in \mathbb{N}.$$

1. Montrez que R est un ordre partiel large.
2. Montrez que R n'est pas un ordre total.
3. Montrez que $\mathcal{F}$ possède un plus petit élément f_0, c'est-à-dire $f_0 R f$ pour tout $f \in \mathcal{F}$.

Exercice 116 (Combinatoire et probabilités)
Une application sécurisée demande la saisie d'un mot de passe composé de six chiffres (c'est-à-dire six valeurs entre 0 et 9).

1. Soit N l'ensemble des mots de passe. Donnez la cardinalité de N.
2. Soit N_1 l'ensemble des mots de passe composés avec six chiffres différents.
   Calculez la cardinalité de N_1.
3. Soit N_2 l'ensemble des mots de passe composés avec cinq chiffres différents. Nous avons donc un chiffre qui apparaît deux fois.
   Calculez la cardinalité de N_2.
4. Soit N_3 l'ensemble des mots de passe composés avec quatre chiffres différents et où deux chiffres apparaissent deux fois.
   Calculez la cardinalité de N_3.
5. Soit N_4 l'ensemble des mots de passe composés avec quatre chiffres différents et où un chiffre apparaît trois fois.
   Calculez la cardinalité de N_4.
6. On suppose que l'on génère le mot de passe avec la distribution uniforme.
   Donnez l'espace de probabilité. Calculer la probabilité d'un évènement en fonction de sa cardinalité.

7. Calculez p_1 (resp. p_2, p_3) la probabilité d'obtenir un mot à six chiffres (resp. cinq et quatre).

Exercice 117 (Ensembles, produit scalaire)

1. Soient A et B deux ensembles.
   Redonnez la définition de $A \times B$ et $A \cap B$.
2. Montrez que l'on a l'égalité suivante

$$(A \times B) \cap (B \times A) = (A \cap B) \times (A \cap B).$$

Exercice 118 (induction sur les arbres)

1. Redonnez la définition inductive des arbres binaires `l.c.` (localement complets).

   On définit inductivement une fonction C sur les arbres binaires par
   (i) Si A est l'arbre vide alors $C(A) = 0$, si A est l'arbre racine alors $C(A) = 1$.
   (ii) Soient B et C deux arbres binaires et $A = (\cdot, B, C)$.
   $C(A) = C(B) \oplus C(C)$ (somme modulo 2).

   Nous noterons $N(A)$ le nombre de nœuds d'un arbre A.
2. Montrez que pour tout arbre `l.c.` nous avons

$$\begin{aligned} C(A) &= 0, \text{ lorsque } N(A) \text{ est pair} \\ &= 1, \text{ lorsque } N(A) \text{ est impair} \end{aligned}$$

Exercice 119 (Probabilités, variables discrètes)
On jette un dé à six faces numérotées de 1 à 6.
On associe à cette expérience aléatoire une variable aléatoire X telle que $X = 1$ lorsque le résultat est $1, 2, 3$ ou 4 et $X = 3$ lorsque le résultat est 5 ou 6.

1. Donnez D, l'espace de probabilité.
   On suppose que nous avons la distribution uniforme sur D.
   Quelle est la probabilité d'un évènement de E ?
2. Donnez la distribution de probabilité de X.
   Calculez l'espérance et la variance de X.
3. On suppose que X correspond au gain d'un joueur que la banque doit lui verser lorsqu'il joue une fois. Quelle somme ce joueur doit-t-il miser à la banque à chaque fois afin que le jeu soit équitable entre ce joueur et la banque ?