Mathématiques discrètes et applications à l'informatique
Polycopié d'exercices

Licence d'informatique deuxième année

2019-2020

Table des matières

1 Inductions sur les arbres binaires

Exercice 1 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. On prendra -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 :

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

Exercice 2 Arbres binaires filiformes
Un arbre binaire dégénéré ou filiforme est un arbre de hauteur $n-1$ à n nœuds.
Trouvez un shéma d'induction des arbres filiformes.

Exercice 3 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 le 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 4 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 un schéma d'induction pour construire l'ensemble des arbres binaires localement complets.
2. Soit A un arbre binaire localement complet. Montrez par induction que A possède un nombre impair de nœuds.
3. 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 5 Arbres parfait et quasi parfaits
Un arbre binaire est dit parfait ou presque complet lorsque tous les niveaux sont entièrement remplis sauf éventuellement le dernier niveau, et dans ce cas, les feuilles du dernier niveau sont regroupées le plus à gauche possible.
Un arbre binaire est quasi parfait lorsque tous les niveaux sont entièrement remplis sauf le dernier niveau où aucune condition n'est imposée.

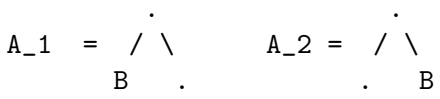
1. Donnez un schéma d'induction de l'ensemble des arbres binaires quasi parfaits.

2. Calculez le nombre d'arbres binaires parfaits et quasi parfaits de hauteur h (h entier positif).

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 $\mathcal{D}$:



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
Soit A un arbre binaire, on rappelle la définition inductive de $h(A)$, la hauteur de A :

(i) Si A est l'arbre vide, $h(A) = -1$.

(ii) Si $A = (\cdot, B, C)$ où B est le sous-arbre gauche et C est le sous-arbre droit, alors $h(A) = 1 + \max(h(B), h(C))$.

1. Redonnez le schéma d'induction des arbres complets.
2. On attribue une valeur à chacun des nœuds des arbres complets 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.
3. Donnez les valeurs de nœuds de l'arbre complet de hauteur 3.
4. Montrez par induction que tout arbre complet 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 :

— $B = \{(i, i)/i \in E\}$
— $C = \{(i, j)/i \in F, j \in E\}$
— $D = \{(i, j)/i \in E, j \in F\}$

1. Représentez A par une grille.
2. 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

i) $A \cap B \subset A \cap C$.
ii) $A \cup B \subset A \cup C$.

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 $\complement A$ le complémentaire de A dans E.

1. Montrez que $A \subset B$ implique $\complement B \subset \complement A$

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

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

$$A \cap B = A \cap C \Rightarrow A \cap \complement B = A \cap \complement C.$$

Exercice 17 Session1 2018-2019
Soient E un ensemble et A, B et C deux sous-ensembles de E. Nous noterons $\overline{A}$ le complémentaire de A dans E et utiliserons la même notation pour tout sous-ensemble 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 dans le cas positif et donnerez un contre-exemple dans le cas négatif). 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 ?

Exercice 22 Session2 2018-2019
On considère la fonction f de $\mathbb{R}\times\mathbb{R}$ vers $\mathbb{R}\times\mathbb{R}$ définie par

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

1. Montrez que f est une bijection. Vous donnerez la fonction réciproque f^{-1}.
2. 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.

Exercice 23 Session2 2018-2019

1. Soit f une application d'un ensemble A dans un ensemble B. Donner la définition de « f est injective » et de « f est surjective ».
2. On considère les fonctions f , g et h de $\mathbb{R}^2$ vers $\mathbb{R}^2$ définies par :

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

— Est-ce que f et g sont injectives ? surjectives ?
— 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 24
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 25
Dans une université, un ensemble d'étudiants E peut choisir des activité sportives 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 26 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 et d'un 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 une relation d'ordre ? Si oui l'ordre est-il large ou strict ? partiel ou total ?

Exercice 27 Modulo et classes d'équivalences
Soit n un entier. 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 28 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 29 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 30 CC 2018-2019
On considère la relation $\mathcal{R}$ définie sur $\mathbb{Z} \times \mathbb{N}^*$ par :

$$(p, q)\mathcal{R}(p', q') \Leftrightarrow pq' = p'q.$$

Montrer que $\mathcal{R}$ est une relation d'équivalence.

Exercice 31 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 32 Session1 2018-2019
Dans $\mathbb{N}$, on définit une relation $<<$ par : $x << y$ s'il existe $m \in \mathbb{N}$ tel que $y = mx$.
Montrer que est une relation d'ordre partiel sur $\mathbb{N}$.

Exercice 33 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. Montrer que R est une relation d'équivalence.
3. On désigne par $[(p, q)]$ la classe d'équivalence de (p, q). Déterminer les ensembles F et G tels que $[(1, 2)] = F \times G$.

Exercice 34 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 par :
   $R = \{(a, b), (c, a), (b, d), (c, d), (c, b), (a, d)\}$
   Montrer que R est une relation d'ordre. Si oui l'ordre est-il large ou strict ? partiel ou total ?

Exercice 35 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 36 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.
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 37 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 stricte, partielle ou totale).
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 38 Principe des choix succcessifs
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 ?
   Pour des raisons diététiques, on interdit certaines combinaisons.
2. Combien de menus sans frites ni charcuterie peut-on composer ?
3. Combien de menus sans œufs ni crème caramel peut-on composer ?

Exercice 39 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 $\mathcal{A} = \{a, b\}$.

3. le nombre de fonctions booléennes à n variables.

Exercice 40 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 full (un brelan et une paire).
6. Calculez le nombre de carré (quatre cartes de la même hauteur)

5.2 Coefficients binomiaux

Exercice 41 **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 42 **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 43 **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 44 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 45 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 46 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 47 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 48 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 49
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 50 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 ?

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 51 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 52 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 53 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 54 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 55 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 LL ni SS ?

Exercice 56 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 57 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 58 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 59 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).

5.7 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 60 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.

6 Probabilités discrètes

6.1 Exercices de base

Exercice 61 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 62 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 63 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 64 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 65
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 66 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 Probabilités et QCM

Exercice 67 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 ?

6.3 Annales

Exercice 68 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 69 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 ?

6.4 Cryptographie

Exercice 70 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.

6.5 Codes correcteurs d'erreur

Deux personnes souhaitent communiquer entre-elles. Elles commencent par choisir un canal de communication. Ensuite, l'émetteur envoie un message au destinataire via ce canal de communication. Il peut arriver que du bruit altère ce message. Il est donc important de pourvoir détecter et/ou

corriger les erreurs induites par ce bruit. Les codes correcteurs permettent de résoudre ce problème en ajoutant de la redondance au message.

Soit k et $n \in \mathbb{N}$ avec $k < n$. Le message de départ est une suite binaire $m = (m_1, \ldots, m_k)$. Il est encodé par un message $c = (c_1, \ldots, c_n)$ calculé à partir de m et c'est ce message qui est envoyé par le canal de communication.

Exercice 71 Bit de parité
On fixe $k \in \mathbb{N}$ et $n = k + 1$. Soit $m = (m_1, \ldots, m_k)$ et $c = (c_1, \ldots, c_{k+1})$ tel que

$$\begin{array}{lcl} c_1 & = & m_1, \\ \vdots & = & \vdots \\ c_k & = & m_k, \\ c_{k+1} & = & m_1 \oplus \ldots \oplus m_k. \end{array}$$

c_{k+1} est appelé le bit de parité de m.

1. Donnez la matrice M qui permet de passer de m à c.
2. Montrez que si nous avons une seule erreur sur c alors le bit de parité est faux, c'est-à-dire $c_{k+1} \neq m_1 \oplus \ldots \oplus m_k$. Montrez qu'en revanche avec deux erreurs le bit de parité reste vrai.
3. On suppose que chaque bit de c a une probabilité ε d'être modifié lors de la transmission. Soit $t \in \mathbb{N}$, $1 \leq t \leq k + 1$. Calculez la probabilité d'avoir t erreurs, nous noterons $p(t)$ cette probabilité.
4. Considérons $k = 20$ et $\varepsilon = 10^6$. On admettra que la probabilité d'avoir plus de 2 erreurs est négligeable. Quelle est la probabilité de ne pas détecter des erreurs ?

Exercice 72 Répétitions
On fixe $k \in \mathbb{N}$ et $n = 3k$. Soit $m = (m_1, \ldots, m_k)$ et $c = (c_1, \ldots, c_{3k})$ tel que $c_1 = c_2 = c_3 = m_1, c_4 = c_5 = c_6 = m_2, \ldots$. On décompose c en blocs de taille 3, $c = (C_1, \ldots, C_k)$. Le destinataire décode c en prenant la valeur majoritaire pour chaque bloc (1 si le bloc contient la valeur 1 2 ou 3 fois, 0 sinon).

1. Donnez la matrice M qui permet de passer de m à c.
2. Montrez que l'on peut corriger une erreur s'il y a une seule erreur sur un bloc.
3. On suppose que chaque bit de c a une probabilité ε d'être modifié lors de la transmission. Soit $i \in \{1, \ldots, k\}$, quelle est la probabilité de faire une erreur sur m_i ? Quelle est la probabilité de ne faire aucune erreur ?

Exercice 73 Protocole HB d'authentification
Le protocole d'authentification HB suivant a été proposé par Hopper et Blum en 2000. Il a été conçu afin d'éviter l'utilisation d'un mot de passe dans le cas où les communications peuvent être interceptées. L'introduction d'erreurs permet de garantir la sécurité du système au détriment de l'utilisabilité (le protocole ne marche pas à tous les coups, car A n'est pas sûr d'être authentifié).

Soit k et $r \in \mathbb{N}$ fixés. Une personne A s'authentifie à un serveur S de la manière suivante. La personne et le serveur se mettent d'accord sur un secret $s = s_1 \ldots s_k$ qui est une suite binaire de longueur k pour un certain entier k fixé.

Une étape Le serveur S envoie à A une suite binaire $c = c_1 \ldots c_k$ générée aléatoirement. A renvoie le bit $b = c \cdot s = c_1 s_1 \oplus c_2 s_2 \oplus \ldots \oplus c_n s_n$. S accepte la réponse lorsque $c \cdot s = b$.

Protocole complet L'authentification est faite lorsque r étapes successives sont faites avec succès.

Une personne B essaie de s'authentifier sans connaître le secret s. Pour cela, elle envoie des bits b au hasard.

1. Quelle est la probabilité qu'elle réussisse une étape ?
2. Quelle est la probabilité qu'elle arrive à s'authentifier ?
3. B arrive à se faire passer pour le serveur S. Quelle suite c doit-elle envoyer à A pour trouver la valeur s_1 ? En déduire une méthode pour retrouver le secret s dans sa totalité.
4. On ajoute maintenant une erreur e, avec $0 < e < 1$. A chaque étape i, A renvoie le bit $d_i = c \cdot s = c_1 s_1 \oplus c_2 s_2 \oplus \ldots \oplus c_n s_n$ avec probabilité $1 - e$ et $1 - d_i$ sinon.
   Quelle est la probabilité que S accepte la réponse en une étape ?
5. Pour le protocole complet S authentifie A lorsque au moins $(1 - e)r$ étapes ont été un succès, où r est un paramètre du protocole.
   Quelle est la probabilité que A réussisse à s'authentifier ? Faites le calcul pour $k = r = 10$ et $e = \frac{1}{4}$.
6. Quelle est la probabilité que B réussisse à s'authentifier avec ce nouveau protocole si elle envoie des bits b au hasard ? Comparez avec le premier protocole.
7. En reprenant la méthode de la question 3, quelle la probabilité que B puisse trouver s_1 en envoyant une seule suite c ? Quel protocole vous semble le meilleur ?