

Synthèse Ultime

LEPL1108 — Mathématiques discrètes et probabilités

UCLouvain — Quadrimestre 3

O. De Baerdemaker

Orientée résolution de problèmes

Avant-propos

Salut à toi, vaillant(e) étudiant(e) en plein blocus de **Mathématiques Discrètes et Probabilités** !

Si tu as ce document sous les yeux (peut-être à 2h du matin avec un café tiède la veille de l'examen), voilà le topo : je suis un profil **ultra-visuel**. J'ai un besoin viscéral de clarté, de schémas, de codes couleurs et de structures bien nettes... tout en ayant un esprit, soyons honnêtes, parfois un peu (beaucoup) éparpillé.

Quand je me suis retrouvé face au cours de LEPL1108 — jonglant entre les graphes planaires, les théorèmes de Lagrange, les nombres de Stirling, la formule d'inversion de Bayes, le théorème central limite et les fonctions génératrices — il me fallait absolument un moyen de transformer ce grand puzzle en quelque chose de limpide, logique et directement actionnable le jour J.

Cette synthèse a donc été construite sur mesure comme une **boîte à outils de terrain** :

- Des **boîtes thématiques colorées** pour repérer en un clin d'œil les définitions clés, les théorèmes directeurs et surtout les **pièges classiques d'examen** où l'on perd bêtement des points précieux.
- Des **procédures de résolution pas-à-pas** pour chaque grand type d'exercice d'examen : plus besoin d'hésiter devant sa feuille en se demandant par quel bout attaquer l'énoncé.
- Des **arbres décisionnels TikZ** pour guider instantanément le choix de la bonne méthode dès la lecture de l'exercice.
- Une priorité donnée à l'**intuition visuelle et graphique**, appuyée par les schémas authentiques extraits des examens officiels et des cours magistraux.
- Des **exemples réels entièrement résolus** tirés directement des sessions d'examens récentes (2021 à 2026).

Prends ce qui t'aide, annote, surligne et approprie-toi chaque méthode. Ce cours peut paraître impressionnant par sa diversité, mais avec de la méthode, du repérage visuel et un entraînement ciblé, il se dompte à merveille.

Je te souhaite un maximum d'énergie, des révisions productives et surtout : **déchire tout à tes examens !**

O. De Baerdemaker

Table des matières

Avant-propos	2
1 Théorie des Graphes & Algorithmes de Réseau	4
1.1 Rappels théoriques	4
1.2 Procédures de résolution	6
2 Structures Algébriques & Cryptographie Moderne	10
2.1 Rappels théoriques	10
2.2 Procédures de résolution	12
3 Dénombrement Combinatoire & Approximation de Stirling	15
3.1 Rappels théoriques	15
3.2 Procédures de résolution	17
4 Fondements des Probabilités & Conditionnement	19
4.1 Rappels théoriques	19
4.2 Procédures de résolution	20
5 Variables Aléatoires & Lois Usuelles (Discrètes et Continues)	23
5.1 Rappels théoriques	23
5.2 Procédures de résolution	25
6 Espérance, Variance & Théorèmes de Concentration	28
6.1 Rappels théoriques	28
6.2 Procédures de résolution	29
7 Fonctions Génératrices & Applications Stochastiques	32
7.1 Rappels théoriques	32
7.2 Procédures de résolution	33
8 Méthodes transversales & Réflexes d'examen	37
8.1 Les <i>Red Flags</i> : signes que vous êtes sur la mauvaise piste	37
8.2 L'Arbre Décisionnel Ultime Transversal	38
8.3 Vérifications de bon sens (<i>Sanity Checks</i>)	38

1 Théorie des Graphes & Algorithmes de Réseau

Les graphes modélisent toute relation binaire sur un ensemble : réseaux de communication, circuits, dépendances logiques, tournois ou cartes routières. En examen, ce chapitre représente systématiquement une question majeure sous forme d'application algorithmique (Kruskal, Dijkstra), de test de planarité, de comptage de marches ou d'analyse structurelle (degrés, arbres, tournois). La clé de voûte : traduire une propriété globale de connexité ou de parité en un calcul local immédiat (degrés, matrices).

1.1 Rappels théoriques

Définition – Graphe, Sommets, Arêtes et Degrés

Un **graphe** $G = (V, E)$ est constitué d'un ensemble fini de sommets (nœuds) V ($|V| = n$ est l'**ordre**) et d'un ensemble fini d'arêtes E ($|E| = m$ est la **taille**).

- **Graphe simple** : sans boucle (arête reliant un sommet à lui-même) ni arêtes multiples entre deux sommets.
- **Degré** $\deg(v)$: nombre d'arêtes incidentes à v (une boucle compte pour 2).
- **Graphe orienté** : les arêtes sont des couples ordonnés $(u, v) \in V \times V$. On distingue le degré sortant $\deg^+(v)$ et le degré entrant $\deg^-(v)$.

Théorème – Lemme des Poignées de Mains (Handshaking Lemma)

Pour tout graphe non orienté $G = (V, E)$:

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

Corollaire immédiat d'examen : La somme des degrés est toujours **paire**. Le nombre de sommets de degré impair est obligatoirement **pair**.

Définition – Parcours, Chaînes, Cycles et Connexité

- **Chaîne (Walk/Path)** : suite alternée de sommets et d'arêtes reliant u à v .
- **Chaîne simple** : ne passant jamais deux fois par le même sommet.
- **Cycle** : chaîne fermée d'au moins 3 sommets distincts dont seul le point de départ et d'arrivée coïncide.
- **Connexité** : G est connexe s'il existe une chaîne entre toute paire de sommets.

Théorème – Théorème d'Euler pour les Pistes et Circuits Eulériens

Soit G un graphe connexe (ou dont les sommets isolés sont ignorés) :

- G admet un **circuit eulérien** (cycle passant exactement une fois par chaque arête) si et seulement si **tous ses sommets ont un degré pair**.
- G admet une **piste eulérienne ouverte** (reliant deux sommets distincts en parcourant chaque arête une fois) si et seulement si **exactement deux sommets ont un degré impair** (les extrémités de la piste).

Théorème – Caractérisation des Arbres, Forêts, Isthmes et DAG

Pour un graphe simple $G = (V, E)$ d'ordre $|V| = n$:

- Caractérisations équivalentes d'un arbre** :
 - G est connexe et sans cycle.
 - G est connexe et possède exactement $n - 1$ **arêtes** ($|E| = n - 1$).
 - G est sans cycle et possède exactement $n - 1$ **arêtes**.

- Il existe une unique chaîne simple entre toute paire de sommets.
- G est minimalement connexe (supprimer une arête quelconque détruit la connexité).
- G est maximalement acyclique (ajouter une arête crée un unique cycle).

(ii) **Relation d'Euler pour une forêt** : Si G est une forêt sans cycle composée de c composantes connexes :

$$|E| = |V| - c$$

(iii) **Isthme (Arête critique)** : Une arête $e \in E$ est un isthme si et seulement si sa suppression augmente strictement le nombre de composantes connexes.

$$e \text{ est un isthme} \iff e \text{ n'appartient à aucun cycle de } G$$

(iv) **Théorème des DAG (Graphes orientés acycliques)** : Tout graphe orienté acyclique fini non vide possède **au moins une source** ($\deg^-(s) = 0$) et **au moins un puits** ($\deg^+(p) = 0$). Tout DAG admet un ordre topologique (numérotation respectant le sens des arcs).

Théorème – Caractérisation des Graphes Bipartis et 2-Coloration

Un graphe $G = (V, E)$ est dit **biparti** s'il existe une partition des sommets $V = V_1 \cup V_2$ ($V_1 \cap V_2 = \emptyset$) telle que chaque arête relie un sommet de V_1 à un sommet de V_2 (aucune arête interne à V_1 ou V_2).

$$G \text{ est biparti} \iff G \text{ ne contient aucun cycle de longueur impaire} \iff G \text{ est 2-coloriable}$$

Algorithme de 2-coloration par parcours BFS : On initialise la racine avec la couleur 0, puis chaque voisin non visité reçoit la couleur opposée $1 - c$. Si deux sommets adjacents reçoivent la même couleur, le graphe n'est pas biparti (cycle impair détecté).

Théorème – Propriétés Fondamentales des Coupes et des Cycles

Soit $G = (V, E)$ un graphe connexe. Pour toute partie non vide de sommets $S \subset V$, la **coupe** (ou cocycle) associée est l'ensemble des arêtes traversantes $\delta(S) = \{\{u, v\} \in E \mid u \in S, v \notin S\}$.

- **Orthogonalité Coupe-Cycle** : Pour tout cycle C et toute coupe $\delta(S)$, le nombre d'arêtes partagées est **toujours pair** :

$$|C \cap \delta(S)| \equiv 0 \pmod{2}$$

- **Cycles et Coupes fondamentaux** : Étant donné un arbre couvrant T de G :
 - L'ajout de toute arête $e \in E \setminus T$ crée un unique cycle dit **cycle fondamental** $C(T, e) \subseteq T \cup \{e\}$.
 - La suppression de toute arête $e \in T$ scinde T en deux composantes définissant une **coupe fondamentale** $\delta(T, e)$.

Théorème – Formule d'Euler et Planarité

Un graphe est **planaire** s'il peut être dessiné dans le plan sans que ses arêtes ne se croisent. Pour tout graphe connexe planaire ayant V sommets, E arêtes et découpant le plan en F faces (y compris la face extérieure non bornée) :

$$V - E + F = 2$$

Si $V \geq 3$ et sans faces de longueur 1 ou 2, chaque face a au moins 3 arêtes frontières ($2E \geq 3F$), d'où :

$$E \leq 3V - 6$$

Corollaire : Le graphe complet K_5 ($V = 5, E = 10 > 3(5) - 6 = 9$) et le graphe biparti complet $K_{3,3}$ ($E = 9 > 2(6) - 4 = 8$) ne sont **pas planaires**.

Propriété – Représentations Matricielles, Comptage de Marches et Isomorphisme

1. **Matrice d'Adjacence** A : $A_{ij} = 1$ si $\{i, j\} \in E$, 0 sinon.

$$(A^k)_{ij} = \text{nombre de parcours (marches) de longueur exactement } k \text{ reliant } i \text{ à } j$$

Le nombre total de triangles dans G est donné par $\frac{1}{6} \text{Tr}(A^3)$.

2. **Matrice Laplacienne** L : Définie par $L = D - A$, où $D = \text{diag}(\deg(v_1), \dots, \deg(v_n))$.

- L est symétrique semi-définie positive, la somme de chaque ligne est nulle ($L\mathbf{1} = \mathbf{0}$).
- Le nombre de composantes connexes de G est égal à la multiplicité de la valeur propre 0.

3. **Complexités spatiales comparées :**

- **Matrice d'adjacence** : Espace $\mathcal{O}(|V|^2)$. Test d'adjacence en temps immédiat $\mathcal{O}(1)$. Idéal pour graphes denses.
- **Listes de voisins (adjacence)** : Espace compact $\mathcal{O}(|V| + |E|)$. Idéal pour graphes creux ($|E| \ll |V|^2$).

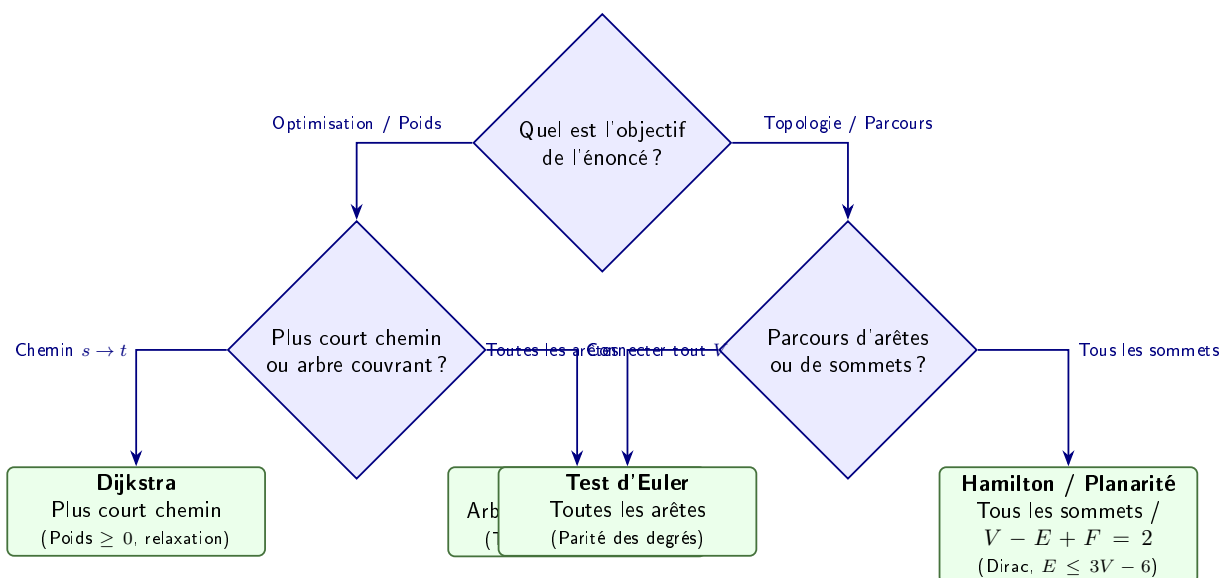
4. **Isomorphisme de graphes** : Deux graphes G_1 et G_2 sont **isomorphes** ($G_1 \cong G_2$) s'il existe une bijection $\phi : V_1 \rightarrow V_2$ préservant les arêtes, c'est-à-dire s'il existe une matrice de permutation P telle que :

$$A_2 = P A_1 P^T$$

Invariants d'isomorphisme clés (pour prouver le non-isomorphisme) : Même nombre de sommets et d'arêtes, même suite ordonnée des degrés, même spectre de valeurs propres de A et L , même nombre de triangles et même diamètre.

1.2 Procédures de résolution

1.2.1 Arbre décisionnel : quel outil de graphe utiliser ?



1.2.2 Fiches de procédure opérationnelle

Procédure : Arbre Sous-tendant de Poids Minimum par Kruskal

Donnée : Un graphe connexe pondéré $G = (V, E, w)$ à $n = |V|$ sommets.

Étape 1 Tri préalable : Lister l'ensemble des arêtes E par ordre croissant de poids : $w(e_1) \leq w(e_2) \leq \dots \leq w(e_m)$ (les poids négatifs sont parfaitement autorisés!).

Étape 2 Initialisation : Initialiser l'arbre $T = \emptyset$ et un compteur d'arêtes sélectionnées $k = 0$.

Étape 3 Sélection gloutonne : Parcourir les arêtes triées une par une :

- Si l'ajout de l'arête e à T **ne crée aucun cycle**, alors poser $T \leftarrow T \cup \{e\}$ et $k \leftarrow k + 1$.
- Sinon, rejeter définitivement l'arête e .

Étape 4 Condition d'arrêt : Stopper dès que $k = n - 1$. Le poids total de l'arbre optimal est la somme des poids des $n - 1$ arêtes retenues.

Procédure : Plus Court Chemin par Dijkstra

Donnée : Un graphe orienté ou non $G = (V, E, w)$ avec $w(e) \geq 0$ pour toute arête, et un sommet source $s \in V$.

Étape 1 Initialisation : Fixer $d(s) = 0$ et $d(v) = +\infty$ pour tout $v \neq s$. Définir l'ensemble des sommets non visités $U = V$.

Étape 2 Sélection : Choisir le sommet $u \in U$ minimisant $d(u)$.

Étape 3 Relaxation des voisins : Pour chaque voisin $v \in U$ de u :

$$d(v) \leftarrow \min(d(v), d(u) + w(u, v))$$

Étape 4 Marquage : Retirer u de U (u est définitivement fixé). Répéter jusqu'à ce que $U = \emptyset$ ou que la cible soit atteinte.

Attention – Pièges classiques d'examen sur les Graphes

- **Dijkstra et poids négatifs :** Dijkstra est **strictement invalide** dès lors qu'au moins une arête possède un poids négatif ! Dans ce cas, il faut utiliser l'algorithme de **Bellman-Ford** (complexité $\mathcal{O}(|V||E|)$). En revanche, **Kruskal gère les poids négatifs sans aucune modification**.
- **Confusion Eulérien vs Hamiltonien :** Eulérien = passe une fois par chaque **arête** (facile, test immédiat de parité des degrés) ; Hamiltonien = passe une fois par chaque **sommet** (problème NP-complet en général).
- **Planarité et composantes :** La formule $V - E + F = 2$ n'est valable que pour un graphe **connexe**. Pour un graphe à k composantes connexes : $V - E + F = 1 + k$.

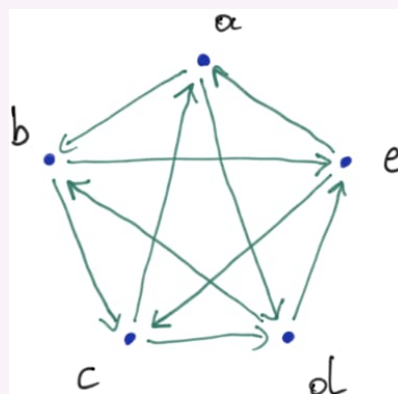
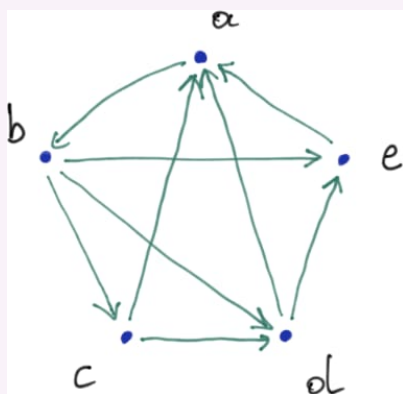
Astuce – Raccourcis d'examen express

- **Arrêt éclair de Kruskal :** Dès que tu as sélectionné $|V| - 1$ arêtes, **arrête immédiatement l'examen des arêtes restantes**, même s'il en reste des dizaines. L'arbre est obligatoirement complet.
- **Roi d'un tournoi :** Dans un tournoi (graphe complet orienté où pour toute paire $\{u, v\}$, soit $(u, v) \in R$ soit $(v, u) \in R$), **le sommet ayant le degré sortant maximal est TOUJOURS un roi** (il atteint tous les autres à distance ≤ 2).

1.2.3 Exemples résolus réels tirés des examens

Exemple – Examen Janvier 2025, Question 1 : Le Roi de la basse-cour

Contexte : Soit un tournoi $G = (V, R)$ modélisant la domination entre poulets : pour tout couple $\{a, b\}$, soit $(a, b) \in R$, soit $(b, a) \in R$. Un sommet a est **roi** si tout autre sommet b vérifie $b \in D_1(a) \cup D_2(a)$ (distance ≤ 2).



Questions et résolutions intégrales :

- (a) Dessiner un tournoi à 5 sommets contenant un roi a ne dominant qu'un unique autre sommet ($\deg^+(a) = 1$).

Résolution : On choisit a dominant uniquement b ($\deg^+(a) = 1$). Pour que a soit roi, b doit dominer tous les autres sommets $\{c, d, e\}$. Ainsi $c, d, e \in D_2(a)$. Comme a ne domine que b , les sommets c, d, e dominent tous a . Les relations internes entre c, d, e peuvent être quelconques (ex : cycle $c \rightarrow d \rightarrow e \rightarrow c$).

- (b) Prouver que tout sommet de degré sortant maximal dans un tournoi est toujours roi.

Résolution formelle : Soit a maximisant $\deg^+(a) = |D_1(a)|$. Supposons par l'absurde que a n'est pas roi. Il existe alors un sommet b n'appartenant pas à $D_1(a) \cup D_2(a)$.

- Comme $b \notin D_1(a)$ et G est un tournoi, on a obligatoirement $(b, a) \in R$.
- Comme $b \notin D_2(a)$, b n'est dominé par aucun sommet de $D_1(a)$. Donc pour tout $c \in D_1(a)$, on a $(b, c) \in R$.

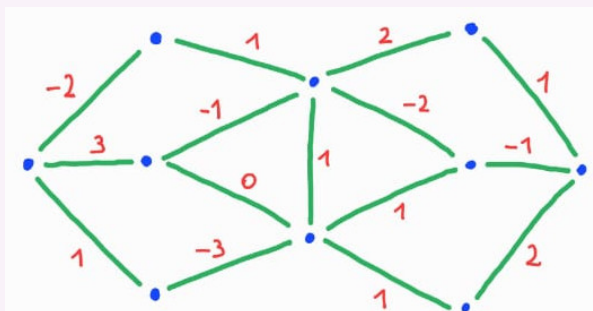
Dès lors, b domine a ainsi que l'ensemble $D_1(a)$. Son degré sortant vérifie :

$$\deg^+(b) \geq 1 + |D_1(a)| = 1 + \deg^+(a) > \deg^+(a)$$

Ce qui contredit formellement la maximalité de $\deg^+(a)$. Donc b ne peut exister et a est obligatoirement roi. $\square$

Exemple – Examen Janvier 2025, Question 3A : Kruskal avec poids négatifs

Énoncé : Calculer le poids minimum d'un arbre sous-tendant pour le graphe de la question 3A (ci-dessous) :



Résolution pas-à-pas : Le graphe compte $n = 6$ sommets. Un arbre sous-tendant doit comporter exactement $n - 1 = 5$ arêtes.

- Tri des arêtes : $-5, -4, -3, 2, 4, 6, \dots$
- Arête 1 : poids -5 (aucun cycle, retenue).
- Arête 2 : poids -4 (aucun cycle, retenue).
- Arête 3 : poids -3 (aucun cycle, retenue).
- Arête 4 : poids 2 (aucun cycle, retenue).
- Arête 5 : poids 4 (connecte le dernier sommet sans cycle, retenue).

On a sélectionné 5 arêtes. On stoppe immédiatement l'algorithme.

$$\text{Poids minimal} = (-5) + (-4) + (-3) + 2 + 4 = \boxed{-6}$$

2 Structures Algébriques & Cryptographie Moderne

Ce chapitre formalise les règles de calcul sur des ensembles abstraits munis d'opérations internes. C'est le socle mathématique de la cryptographie asymétrique (RSA, Diffie-Hellman) et des codes correcteurs d'erreurs (Reed-Solomon). En examen, les questions portent typiquement sur l'ordre d'un élément dans un produit direct, le critère de sous-groupe, l'application du théorème de Lagrange, ou le calcul d'une clé RSA via l'algorithme d'Euclide étendu.

2.1 Rappels théoriques

Définition – Loi Interne, Monoïde, Groupe

Soit E un ensemble muni d'une loi de composition interne $*$: $E \times E \rightarrow E$.

- **Monoïde** : la loi $*$ est **associative** ($a * (b * c) = (a * b) * c$) et possède un **élément neutre** e unique ($\forall a, a * e = e * a = a$).
- **Groupe** $(G, *)$: monoïde où tout élément $a \in G$ admet un **inverse** unique $a^{-1} \in G$ ($a * a^{-1} = a^{-1} * a = e$).
- **Groupe abélien (commutatif)** : si $\forall a, b \in G, a * b = b * a$.

Théorème – Critère Fondamental de Sous-groupe

Une partie non vide $H \subseteq G$ d'un groupe $(G, *)$ est un **sous-groupe** (noté $H \leq G$) si et seulement si :

$$\boxed{\forall x, y \in H, \quad x * y^{-1} \in H}$$

Si H est fini, il suffit que $H \neq \emptyset$ et que H soit stable par la loi : $\forall x, y \in H, x * y \in H$.

Théorème – Théorème de Lagrange

Si G est un groupe fini et H un sous-groupe de G , alors **l'ordre de H divise l'ordre de G** :

$$\boxed{|G| = [G : H] \cdot |H| \implies |H| \text{ divise } |G|}$$

où $[G : H]$ est l'indice de H dans G (nombre de classes latérales à gauche xH).

Définition – Ordre d'un Élément et Groupe Cyclique

L'**ordre** d'un élément $a \in G$, noté $\text{ord}(a)$, est le plus petit entier $k \geq 1$ tel que $a^k = e$.

- Le sous-groupe engendré par a est $\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$, et $|\langle a \rangle| = \text{ord}(a)$.
- **Conséquence de Lagrange** : $\text{ord}(a)$ **divise obligatoirement** l'ordre du groupe $|G|$, et :

$$\boxed{a^{|G|} = e \quad \forall a \in G}$$

- G est **cyclique** s'il est engendré par un unique élément ($G = \langle g \rangle$). Tout groupe cyclique d'ordre n est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.

Théorème – Groupe Symétrique S_n , Décomposition en Cycles et Théorème de Cayley

Soit S_n le groupe des permutations d'un ensemble à n éléments ($|S_n| = n!$).

- **Décomposition en cycles disjoints** : Toute permutation $\sigma \in S_n$ se décompose de manière unique (à l'ordre près) en produit de cycles à supports disjoints. Les cycles disjoints commutent.
- **Ordre d'une permutation** : L'ordre de σ est le plus petit commun multiple des longueurs

de ses cycles disjoints :

$$\text{ord}(\sigma) = \text{ppcm}(\text{longueurs des cycles disjoints})$$

- **Transpositions et Signature** : Toute permutation se décompose en un produit de transpositions (échanges de 2 éléments). La **signature** $\varepsilon(\sigma) \in \{-1, +1\}$ est définie par :

$$\varepsilon(\sigma) = (-1)^{n-c}$$

où c est le nombre total d'orbites (cycles disjoints en comptant les points fixes de longueur 1). Un cycle de longueur L a pour signature $(-1)^{L-1}$.

- **Théorème de Cayley** : Tout groupe fini G d'ordre n est isomorphe à un sous-groupe du groupe symétrique S_n .

Théorème – Théorèmes d'Euler et Petit Théorème de Fermat

L'**indicatrice d'Euler** $\phi(n)$ compte les entiers $k \in \{1, \dots, n\}$ tels que $\text{pgcd}(k, n) = 1$. Pour $n = p \cdot q$ avec p, q premiers distincts : $\phi(n) = (p-1)(q-1)$. Si $n = p^k$, $\phi(p^k) = p^{k-1}(p-1)$.

- **Théorème d'Euler** : Si $\text{pgcd}(a, n) = 1$, alors :

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

- **Petit Théorème de Fermat** : Si p est premier et $p \nmid a$, alors :

$$a^{p-1} \equiv 1 \pmod{p} \iff a^p \equiv a \pmod{p}$$

Définition – Anneaux, Algèbres Booléennes et Corps Finis

- **Anneau** $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$: groupe abélien pour $+$, associatif et distributif pour $\cdot$.
- **Anneau Booléen** $(\mathcal{P}(E), \Delta, \cap)$: Muni de la différence symétrique Δ (addition) et de l'intersection $\cap$ (multiplication), $(\mathcal{P}(E), \Delta, \cap)$ est un anneau commutatif unitaire :
 - **Caractéristique 2** : $A \Delta A = \emptyset$ (élément nul), donc $A = -A$ (tout élément est son propre opposé).
 - **Idempotence** : $A \cap A = A$ pour tout $A \subseteq E$.
- **Corps** $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$: anneau commutatif où tout élément non nul est inversible pour la multiplication. $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un corps si et seulement si n est **premier**.
- **Groupe multiplicatif** $(\mathbb{Z}/p\mathbb{Z})^*$: d'ordre $p-1$, toujours cyclique.

Propriété – Générateurs de $\mathbb{Z}_p^*$, Racines Primitives et Premiers Sûrs

Le groupe multiplicatif $\mathbb{Z}_p^*$ d'un corps premier $\mathbb{F}_p$ est toujours cyclique d'ordre $p-1$.

- **Nombre de générateurs** : $\mathbb{Z}_p^*$ possède exactement $\phi(p-1)$ générateurs distincts (appelés racines primitives modulo p).
- **Test de racine primitive** : Un élément $g \in \mathbb{Z}_p^*$ est un générateur si et seulement si pour tout diviseur premier q de $p-1$:

$$g^{(p-1)/q} \not\equiv 1 \pmod{p}$$

- **Nombres premiers sûrs (Sophie Germain)** : Si $p = 2q + 1$ où q est un nombre premier impair, les seuls ordres possibles d'éléments non triviaux sont $\{2, q, 2q\}$. Dès lors, pour tout $g \not\equiv \pm 1 \pmod{p}$:

$$g \text{ est générateur de } \mathbb{Z}_p^* \iff g^q \equiv -1 \pmod{p}$$

Théorème – Résidus Quadratiques, Critère d'Euler et Corps de Galois $\mathbb{F}_{p^k}$

- Résidus quadratiques dans $\mathbb{F}_p$** : Un élément non nul $a \in \mathbb{F}_p^*$ est un **résidu quadratique** (un carré) s'il existe $x \in \mathbb{F}_p^*$ tel que $x^2 \equiv a \pmod{p}$. Il y a exactement $\frac{p-1}{2}$ carrés et $\frac{p-1}{2}$ non-carrés dans $\mathbb{F}_p^*$.
- Critère d'Euler (Symbole de Legendre)** :

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \equiv \begin{cases} +1 \pmod{p} & \text{si } a \text{ est un carré dans } \mathbb{F}_p^* \\ -1 \pmod{p} & \text{si } a \text{ n'est pas un carré} \end{cases}$$

Une équation du second degré $ax^2 + bx + c = 0$ ($a \neq 0$) admet des solutions dans $\mathbb{F}_p$ si et seulement si $\Delta = b^2 - 4ac$ vérifie $\left(\frac{\Delta}{p}\right) \in \{0, 1\}$.

- Construction des Corps de Galois $\mathbb{F}_{p^k}$** : Pour tout premier p et tout entier $k \geq 1$, il existe un unique corps fini à p^k éléments, noté $\mathbb{F}_{p^k}$ ou $\text{GF}(p^k)$. On le construit en quotientant l'anneau des polynômes par un **polynôme irréductible** $P(X) \in \mathbb{F}_p[X]$ de degré k :

$$\mathbb{F}_{p^k} \cong \mathbb{F}_p[X]/(P(X))$$

Le groupe multiplicatif $(\mathbb{F}_{p^k})^*$ est cyclique d'ordre $p^k - 1$.

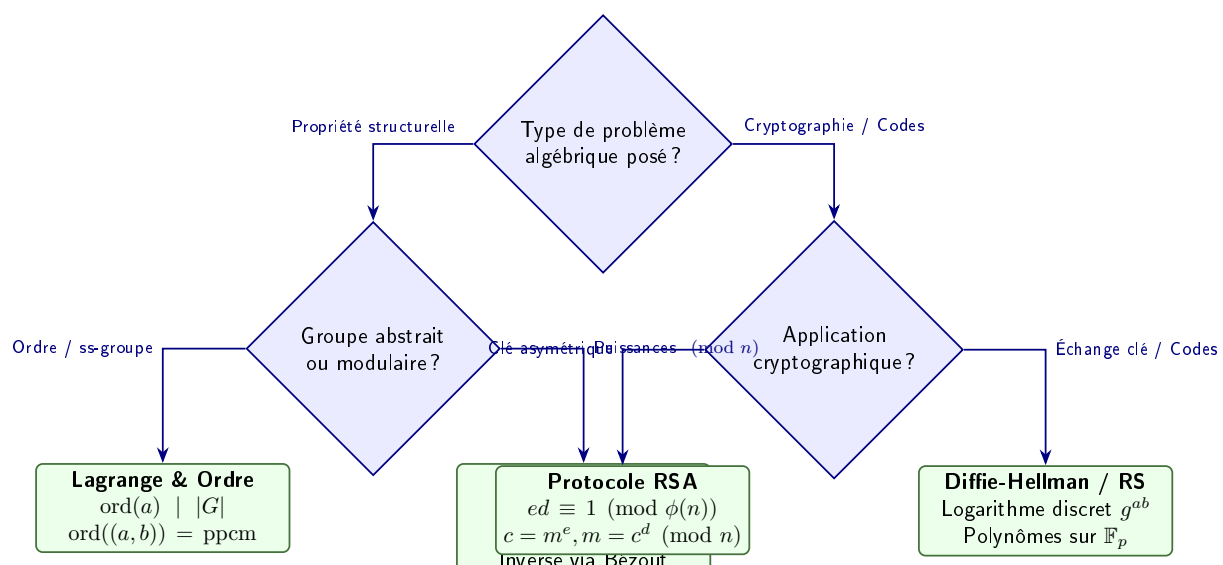
Théorème – Fondements du Cryptosystème RSA

Soient p, q deux grands nombres premiers distincts, $n = pq$, et $\phi(n) = (p-1)(q-1)$.

- Clé publique** : (e, n) où $\text{pgcd}(e, \phi(n)) = 1$.
 - Clé privée** : d tel que $e \cdot d \equiv 1 \pmod{\phi(n)}$ (obtenu par l'algorithme d'Euclide étendu).
 - Chiffrement** : Pour un message $m \in \{0, \dots, n-1\}$, $c \equiv m^e \pmod{n}$.
 - Déchiffrement** : $m \equiv c^d \pmod{n}$.
- Preuve** : $ed = 1 + k\phi(n) \implies c^d \equiv m^{ed} = m \cdot (m^{\phi(n)})^k \equiv m \cdot 1^k \equiv m \pmod{n}$ par Euler-Fermat.

2.2 Procédures de résolution

2.2.1 Arbre décisionnel : quelle structure algébrique utiliser ?



2.2.2 Fiches de procédure opérationnelle

Procédure : Calcul de l'Ordre dans un Produit Direct $G_1 \times G_2$

Donnée : Deux groupes finis G_1, G_2 et un élément $(a, b) \in G_1 \times G_2$.

Étape 1 Calcul individuel des ordres : Déterminer l'ordre $k_1 = \text{ord}(a)$ dans G_1 (plus petit entier tel que $a^{k_1} = e_1$) et $k_2 = \text{ord}(b)$ dans G_2 (plus petit entier tel que $b^{k_2} = e_2$).

Étape 2 Condition de neutralité conjointe : Pour tout entier m :

$$(a, b)^m = (a^m, b^m) = (e_1, e_2) \iff k_1 \mid m \quad \text{et} \quad k_2 \mid m$$

Étape 3 Conclusion : L'ordre de (a, b) est le plus petit multiple commun :

$$\text{ord}((a, b)) = \text{ppcm}(\text{ord}(a), \text{ord}(b))$$

Procédure : Déroulement Complet du Chiffrement / Déchiffrement RSA

Donnée : Les paramètres p, q (premiers), l'exposant public e , et un message m .

Étape 1 Calcul du module et de l'indicatrice : $n = p \cdot q$ et $\phi(n) = (p-1)(q-1)$.

Étape 2 Calcul de la clé privée d : Résoudre $e \cdot d \equiv 1 \pmod{\phi(n)}$ via l'algorithme d'Euclide étendu :

$$e \cdot d + \phi(n) \cdot k = 1$$

Si $d < 0$, ajouter $\phi(n)$ pour obtenir $d \in \{1, \dots, \phi(n) - 1\}$.

Étape 3 Chiffrement : Calculer $c = m^e \pmod{n}$ par exponentiation rapide binaire.

Étape 4 Déchiffrement : Calculer $m = c^d \pmod{n}$.

Procédure : Échange de Clés Diffie-Hellman et Logarithme Discret

Donnée : Un grand nombre premier public p et un générateur public $g \in \mathbb{Z}_p^*$.

Étape 1 Choix des secrets privés : Alice choisit un secret privé $a \in \{1, \dots, p-2\}$. Bob choisit un secret privé $b \in \{1, \dots, p-2\}$.

Étape 2 Échange des clés publiques :

- Alice envoie à Bob la valeur publique $A \equiv g^a \pmod{p}$.
- Bob envoie à Alice la valeur publique $B \equiv g^b \pmod{p}$.

Étape 3 Calcul du secret partagé conjoint :

- Alice calcule $K \equiv B^a \equiv (g^b)^a = g^{ab} \pmod{p}$.
- Bob calcule $K \equiv A^b \equiv (g^a)^b = g^{ab} \pmod{p}$.

Étape 4 Sécurité (Problème du Logarithme Discret) : Un espion connaissant p, g, A, B ne peut pas déduire K sans retrouver a ou b , ce qui nécessite de résoudre $g^x \equiv A \pmod{p}$, problème calculatoirement intraitable pour p grand.

Attention – Pièges classiques d'examen en Algèbre

- **Confusion de module dans RSA :** La base du message est réduite modulo n , mais l'exposant de déchiffrement d est impérativement calculé modulo $\phi(n)$! Ne JAMAIS calculer $ed \equiv 1 \pmod{n}$.
- **Anneau vs Corps :** $\mathbb{Z}/n\mathbb{Z}$ n'est un corps que si n est premier. Si n est composé (ex : $n = 6$), il existe des **diviseurs de zéro** ($2 \cdot 3 \equiv 0 \pmod{6}$) et certains éléments non nuls ne sont pas inversibles.

- **Divisibilité de Lagrange** : Le fait que k divise $|G|$ est une condition **nécessaire** pour qu'un sous-groupe d'ordre k existe, mais **absolument pas suffisante** dans un groupe non abélien quelconque !

Astuce – Raccourcis d'examen express

- **Ordre dans $(\mathbb{Z}/n\mathbb{Z}, +)$** : L'ordre additif de k dans $\mathbb{Z}/n\mathbb{Z}$ est immédiatement $\frac{n}{\text{pgcd}(k,n)}$.
- **Inverse modulaire rapide pour petits nombres** : Pour trouver l'inverse de a modulo m , tester mentalement les valeurs $(k \cdot m + 1)/a$ pour $k = 1, 2, \dots$ jusqu'à obtenir un entier.

2.2.3 Exemples résolus réels tirés des examens

Exemple – Examen Janvier 2025, Question 3B : Produit de groupes cycliques

Énoncé : On considère le groupe additif $G = \mathbb{Z}_5 \times \mathbb{Z}_8$ où l'addition se fait composante par composante : $(2, 3) + (4, 5) = (2 + 4 \bmod 5, 3 + 5 \bmod 8) = (1, 0)$. Combien d'éléments contient le sous-groupe de G engendré par l'élément $(2, 4)$?

Résolution pas-à-pas : Le nombre d'éléments du sous-groupe engendré par un élément est exactement égal à son ordre : $|\langle (2, 4) \rangle| = \text{ord}((2, 4))$.

- Ordre de 2 dans $(\mathbb{Z}_5, +)$: Comme $\text{pgcd}(2, 5) = 1$ et 5 est premier, 2 engendre $\mathbb{Z}_5$, donc $\text{ord}(2) = 5$.
- Ordre de 4 dans $(\mathbb{Z}_8, +)$: On a $4 \neq 0$ et $4 + 4 = 8 \equiv 0 \pmod{8}$, donc $\text{ord}(4) = 2$ (ou $\frac{8}{\text{pgcd}(4,8)} = \frac{8}{4} = 2$).
- L'ordre de $(2, 4)$ dans $G = \mathbb{Z}_5 \times \mathbb{Z}_8$ est donc :

$$\text{ord}((2, 4)) = \text{ppcm}(\text{ord}(2), \text{ord}(4)) = \text{ppcm}(5, 2) = \boxed{10}$$

Le sous-groupe contient donc exactement **10 éléments**.

3 Dénombrement Combinatoire & Approximation de Stirling

Le dénombrement combinatoire est l'art de quantifier exactement le nombre de configurations discrètes sans avoir à les énumérer. C'est la passerelle directe vers le calcul des probabilités uniformes (cas favorables / cas possibles). En examen, les erreurs proviennent quasi exclusivement d'une mauvaise identification de la distinguabilité des objets ou des boîtes, de l'oubli des contraintes de non-vacuité, ou d'une mauvaise gestion des recouvrements résolus par le principe d'inclusion-exclusion.

3.1 Rappels théoriques

Théorème – Dénombrabilité, Bijection de Cantor et Indénombrabilité de $\mathbb{R}$

- (a) **Ensemble dénombrable** : Un ensemble E est dit **dénombrable** s'il est fini ou s'il existe une bijection entre E et $\mathbb{N}$ ($|E| = |\mathbb{N}| = \aleph_0$).
- (b) **Dénombrabilité de $\mathbb{N}^2$ et $\mathbb{Q}$** :
 - $\mathbb{N} \times \mathbb{N}$ est dénombrable via la bijection diagonale de Cantor : $f(x, y) = \frac{(x+y)(x+y+1)}{2} + y$.
 - L'ensemble des rationnels $\mathbb{Q}$ et l'ensemble des mots finis Σ^* sur un alphabet fini sont dénombrables. Toute union dénombrable d'ensembles dénombrables est dénombrable.
- (c) **Indénombrabilité et Argument Diagonal de Georg Cantor (1891)** : L'ensemble des parties $\mathcal{P}(\mathbb{N})$ n'est **pas dénombrable** ($|\mathcal{P}(E)| > |E|$ pour tout ensemble E). Par conséquent, l'ensemble des réels $\mathbb{R}$ et l'intervalle $[0, 1]$ sont strictement **non dénombrables** (ils ont la puissance du continu $\mathfrak{c} = 2^{\aleph_0}$).

Théorème – Règles Fondamentales d'Addition, Multiplication et Tiroirs

- **Règle de la somme** : Si $A_1, \dots, A_k$ sont des ensembles disjoints deux à deux ($A_i \cap A_j = \emptyset$ pour $i \neq j$), alors $|\bigcup_{i=1}^k A_i| = \sum_{i=1}^k |A_i|$.
- **Règle du produit** : Le cardinal d'un produit cartésien de choix indépendants est le produit des cardinaux : $|A_1 \times \dots \times A_k| = \prod_{i=1}^k |A_i|$.
- **Principe des tiroirs généralisé (Dirichlet)** : Si n objets sont placés dans k boîtes, au moins une boîte contient au moins :

$$\left\lceil \frac{n}{k} \right\rceil \text{ objets}$$

Application classique d'examen : Dans toute assemblée de $n \geq 2$ personnes, au moins deux personnes ont exactement le même nombre d'amis dans l'assemblée.

Définition – Les Quatre Configurations de Base (Tirages)

Pour choisir k éléments parmi un ensemble de n éléments distincts :

Type de tirage	Avec ordre	Sans ordre
Sans remise	Arrangements : $A_n^k = \frac{n!}{(n-k)!}$	Combinaisons : $\binom{n}{k} = \frac{n!}{k!(n-k)!}$
Avec remise	Listes : n^k	Étoiles et barres : $\binom{n+k-1}{k}$

Propriété – Propriétés Maîtresses des Coefficients Binomiaux et Règle de Leibniz

- **Symétrie** : $\binom{n}{k} = \binom{n}{n-k}$.

- **Formule de Pascal** : $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$.
- **Formule du binôme de Newton** : $(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k} \implies \sum_{k=0}^n \binom{n}{k} = 2^n$.
- **Formule de Vandermonde** : $\sum_{k=0}^r \binom{m}{k} \binom{n}{r-k} = \binom{m+n}{r}$.
- **Formule de dérivation de Leibniz** : Pour deux fonctions n fois dérivables u et v :

$$(u \cdot v)^{(n)} = \sum_{k=0}^n \binom{n}{k} u^{(k)} v^{(n-k)}$$

- **Réciproques d'applications** : Une fonction $f : E \rightarrow F$ admet une réciproque à gauche si et seulement si f est **injective**. Elle admet une réciproque à droite si et seulement si f est **surjective**.

Théorème – Surjections, Nombres de Stirling et de Bell

Soit $|E| = n$ et $|F| = k$.

- Le nombre de **surjections** de E vers F (noté $\text{Sur}(n \rightarrow k)$ sur le formulaire) est :

$$\text{Sur}(n \rightarrow k) = \sum_{r=0}^k (-1)^r \binom{k}{r} (k-r)^n$$

- Les **nombres de Stirling de seconde espèce** $S(n, k)$ comptent le nombre de façons de partitionner n éléments discernables en k sous-ensembles non vides indiscernables :

$$S(n, k) = \frac{1}{k!} \text{Sur}(n \rightarrow k) = S(n-1, k-1) + k \cdot S(n-1, k)$$

avec $S(n, 1) = 1$, $S(n, n) = 1$, et $S(n, k) = 0$ si $k > n$.

- Les **nombres de Bell** $B_n = \sum_{k=1}^n S(n, k)$ comptent le nombre total de partitions d'un ensemble à n éléments ($B_0 = 1, B_1 = 1, B_2 = 2, B_3 = 5, B_4 = 15$). Ils vérifient la récurrence fondamentale :

$$B_{n+1} = \sum_{k=0}^n \binom{n}{k} B_k$$

Théorème – Principe d'Inclusion-Exclusion et Dérangements

Pour des ensembles finis $A_1, \dots, A_n$:

$$\left| \bigcup_{i=1}^n A_i \right| = \sum_{i=1}^n |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| + \dots + (-1)^{n-1} |A_1 \cap \dots \cap A_n|$$

Dérangements : Le nombre de permutations de $\{1, \dots, n\}$ sans aucun point fixe ($\sigma(i) \neq i$ pour tout i) est :

$$d_n = n! \sum_{r=0}^n \frac{(-1)^r}{r!} \implies \lim_{n \rightarrow \infty} \frac{d_n}{n!} = \frac{1}{e} \approx 0.3679$$

Propriété – Approximation de Stirling et Encadrements (Formulaire Officiel)

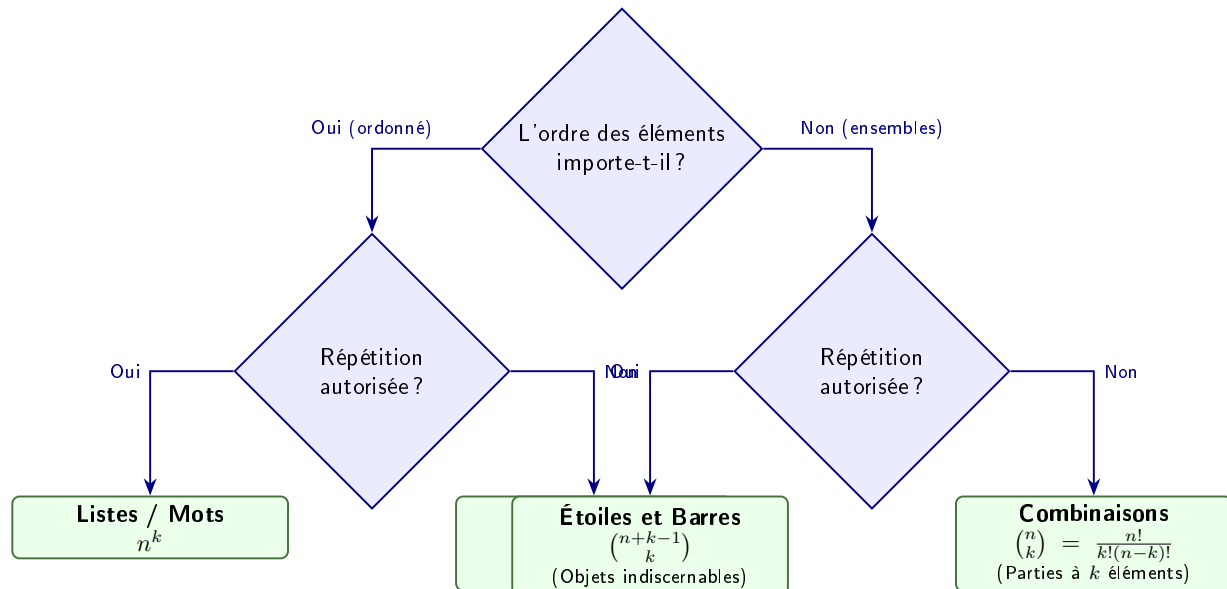
$$\lim_{n \rightarrow \infty} \frac{n!}{\sqrt{2\pi n} (n/e)^n} = 1$$

Encadrements rigoureux figurant sur le formulaire officiel de l'examen :

$$n! \geq \left(\frac{n}{e}\right)^n \quad \text{et} \quad \left(\frac{n}{k}\right)^k \leq \binom{n}{k} \leq \left(\frac{ne}{k}\right)^k$$

3.2 Procédures de résolution

3.2.1 Arbre décisionnel : quelle formule de dénombrement choisir ?



3.2.2 Fiches de procédure opérationnelle

Procédure : Méthode des Étoiles et Barres (Stars and Bars)

Donnée : Trouver le nombre de solutions entières de l'équation $x_1 + x_2 + \dots + x_n = k$.

Étape 1 Cas standard ($x_i \geq 0$) : Placer k étoiles (unités) et $n - 1$ barres (séparateurs entre les n variables). Le nombre de permutations d'un mot de $k + (n - 1)$ symboles contenant k étoiles est :

$$N = \binom{n+k-1}{k} = \binom{n+k-1}{n-1}$$

Étape 2 Cas avec contraintes strictes ($x_i \geq c_i$) : Effectuer le changement de variable $y_i = x_i - c_i \geq 0$. L'équation devient :

$$y_1 + y_2 + \dots + y_n = k - \sum_{i=1}^n c_i =: k'$$

Le nombre de solutions est alors $\binom{n+k'-1}{k'}$. En particulier, si $x_i \geq 1$ (chaque boîte reçoit au moins un objet) : $k' = k - n \Rightarrow \binom{k-1}{n-1}$.

Procédure : Application du Principe d'Inclusion-Exclusion

Donnée : Compter le nombre d'éléments vérifiant au moins l'une des propriétés $P_1, \dots, P_n$.

Étape 1 Définition des ensembles : Poser $A_i = \{\text{éléments vérifiant la propriété } P_i\}$.

Étape 2 Calcul des cardinaux individuels : Déterminer $|A_i|$ pour tout i , puis sommer :

$$S_1 = \sum |A_i|.$$

Étape 3 Calcul des intersections par paires : Déterminer $|A_i \cap A_j|$ pour $i < j$, puis sommer :
 $S_2 = \sum_{i < j} |A_i \cap A_j|.$

Étape 4 Alternance des signes : Poursuivre jusqu'à l'intersection globale :

$$|\bigcup A_i| = S_1 - S_2 + S_3 - \dots + (-1)^{n-1} S_n$$

Étape 5 Passage au complémentaire (si demandé « aucun ne vérifie ») : $|E \setminus \bigcup A_i| = |E| - |\bigcup A_i|.$

Attention – Pièges classiques d'examen en Dénombrement

- **Discernabilité des boîtes et des objets :** Distribuer des billes **identiques** dans des boîtes **distinctes** relève des étoiles et barres ($\binom{n+k-1}{k}$). Distribuer des billes **distinctes** dans des boîtes **identiques** non vides relève de Stirling ($S(n, k)$). Ne jamais confondre !
- **Le piège du sur-comptage :** Choisir d'abord 1 élément pour satisfaire une condition puis choisir le reste induit presque toujours un comptage multiple non maîtrisé. Toujours privilégier la partition en cas disjoints ou le passage au complémentaire.

Astuce – Raccourcis d'examen express

- **Le réflexe complémentaire :** Dès qu'un énoncé contient les termes « *au moins un* » ou « *au plus $n-1$* », calculer systématiquement $N_{\text{total}} - N_{\text{aucun}}$.
- **Dérangements express :** Pour $n \geq 4$, le nombre de dérangements d_n est l'entier le plus proche de $\frac{n!}{e}$: $d_1 = 0, d_2 = 1, d_3 = 2, d_4 = 9, d_5 = 44$.

3.2.3 Exemples résolus réels tirés des examens

Exemple – Examen Août 2023 : Distribution de ressources et surjections

Énoncé : On souhaite distribuer 5 tâches distinctes à 3 serveurs distincts de sorte que **chaque serveur reçoive au moins une tâche**. De combien de manières peut-on réaliser cette affectation ?

Résolution pas-à-pas : Il s'agit d'affecter 5 éléments discernables (E) vers 3 éléments discernables (F) de façon surjective (aucun serveur vide). La réponse est donc le nombre de surjections $\text{Sur}(5 \rightarrow 3)$:

$$\text{Sur}(5 \rightarrow 3) = 3! \cdot S(5, 3)$$

Calculons les nombres de Stirling par la formule de récurrence $S(n, k) = S(n-1, k-1) + k \cdot S(n-1, k)$:

- $S(3, 2) = 3, S(3, 3) = 1.$
- $S(4, 2) = S(3, 1) + 2S(3, 2) = 1 + 2(3) = 7.$
- $S(4, 3) = S(3, 2) + 3S(3, 3) = 3 + 3(1) = 6.$
- $S(5, 3) = S(4, 2) + 3S(4, 3) = 7 + 3(6) = 25.$

Dès lors :

$$\text{Sur}(5 \rightarrow 3) = 3! \cdot 25 = 6 \cdot 25 = \boxed{150}$$

Alternative par inclusion-exclusion (formule du formulaire) :

$$\text{Sur}(5 \rightarrow 3) = \binom{3}{0} 3^5 - \binom{3}{1} 2^5 + \binom{3}{2} 1^5 = 1(243) - 3(32) + 3(1) = 243 - 96 + 3 = \boxed{150}$$

4 Fondements des Probabilités & Conditionnement

Ce chapitre pose les fondations axiomatiques de la théorie des probabilités (Kolmogorov) et introduit l'outil mathématique le plus puissant pour mettre à jour nos croyances face à une nouvelle information : le conditionnement et le théorème de Bayes. En examen, les exercices typiques portent sur les tests médicaux (inversion des probabilités, faux positifs), les probabilités totales et l'analyse de l'indépendance mutuelle.

4.1 Rappels théoriques

Définition – Espace Probabilisé et Axiomes de Kolmogorov

Un **espace probabilisé** est un triplet $(\Omega, \mathcal{F}, \mathbb{P})$ où :

- Ω est l'**univers** des possibles.
- $\mathcal{F}$ est une **σ -algèbre (tribu)** d'événements sur Ω ($\Omega \in \mathcal{F}$, stable par passage au complémentaire et par union dénombrable).
- $\mathbb{P} : \mathcal{F} \rightarrow [0, 1]$ est une **mesure de probabilité** vérifiant les axiomes de Kolmogorov :
 - (i) $\forall A \in \mathcal{F}, \quad 0 \leq \mathbb{P}(A) \leq 1$.
 - (ii) $\mathbb{P}(\Omega) = 1$.
 - (iii) Pour toute suite d'événements disjoints deux à deux ($A_i \cap A_j = \emptyset$) :

$$\mathbb{P}\left(\bigcup_{i=1}^{\infty} A_i\right) = \sum_{i=1}^{\infty} \mathbb{P}(A_i) \quad (\sigma\text{-additivité})$$

Propriété – Propriétés Élémentaires Dédites

- $\mathbb{P}(\emptyset) = 0$ et $\mathbb{P}(A^c) = 1 - \mathbb{P}(A)$.
- Si $A \subseteq B$, alors $\mathbb{P}(A) \leq \mathbb{P}(B)$.
- $\mathbb{P}(A \cup B) = \mathbb{P}(A) + \mathbb{P}(B) - \mathbb{P}(A \cap B)$.
- **Cas équiprobable (Ω fini) :** $\mathbb{P}(A) = \frac{|A|}{|\Omega|} = \frac{\text{nombre de cas favorables}}{\text{nombre de cas possibles}}$.

Définition – Probabilité Conditionnelle et Formule des Chaînes

Pour tout événement B tel que $\mathbb{P}(B) > 0$, la **probabilité conditionnelle** de A sachant B est :

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

Formule des probabilités composées (Règle de la chaîne) :

$$\mathbb{P}(A_1 \cap A_2 \cap \dots \cap A_n) = \mathbb{P}(A_1) \mathbb{P}(A_2 | A_1) \mathbb{P}(A_3 | A_1 \cap A_2) \dots \mathbb{P}(A_n | A_1 \cap \dots \cap A_{n-1})$$

Théorème – Formule des Probabilités Totales et Théorème de Bayes

Soit $(B_1, B_2, \dots, B_n)$ une **partition** de Ω (événements disjoints tels que $\bigcup_{i=1}^n B_i = \Omega$ et $\mathbb{P}(B_i) > 0$).
Pour tout événement A :

- **Probabilités totales :**

$$\mathbb{P}(A) = \sum_{i=1}^n \mathbb{P}(A \cap B_i) = \sum_{i=1}^n \mathbb{P}(A | B_i) \mathbb{P}(B_i)$$

— **Théorème de Bayes (Inversion des probabilités) :**

$$\mathbb{P}(B_k | A) = \frac{\mathbb{P}(A | B_k) \mathbb{P}(B_k)}{\mathbb{P}(A)} = \frac{\mathbb{P}(A | B_k) \mathbb{P}(B_k)}{\sum_{i=1}^n \mathbb{P}(A | B_i) \mathbb{P}(B_i)}$$

Définition – Indépendance d'Événements

Deux événements A et B sont **indépendants** si et seulement si :

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

Si $\mathbb{P}(B) > 0$, cela équivaut strictement à $\mathbb{P}(A | B) = \mathbb{P}(A)$.

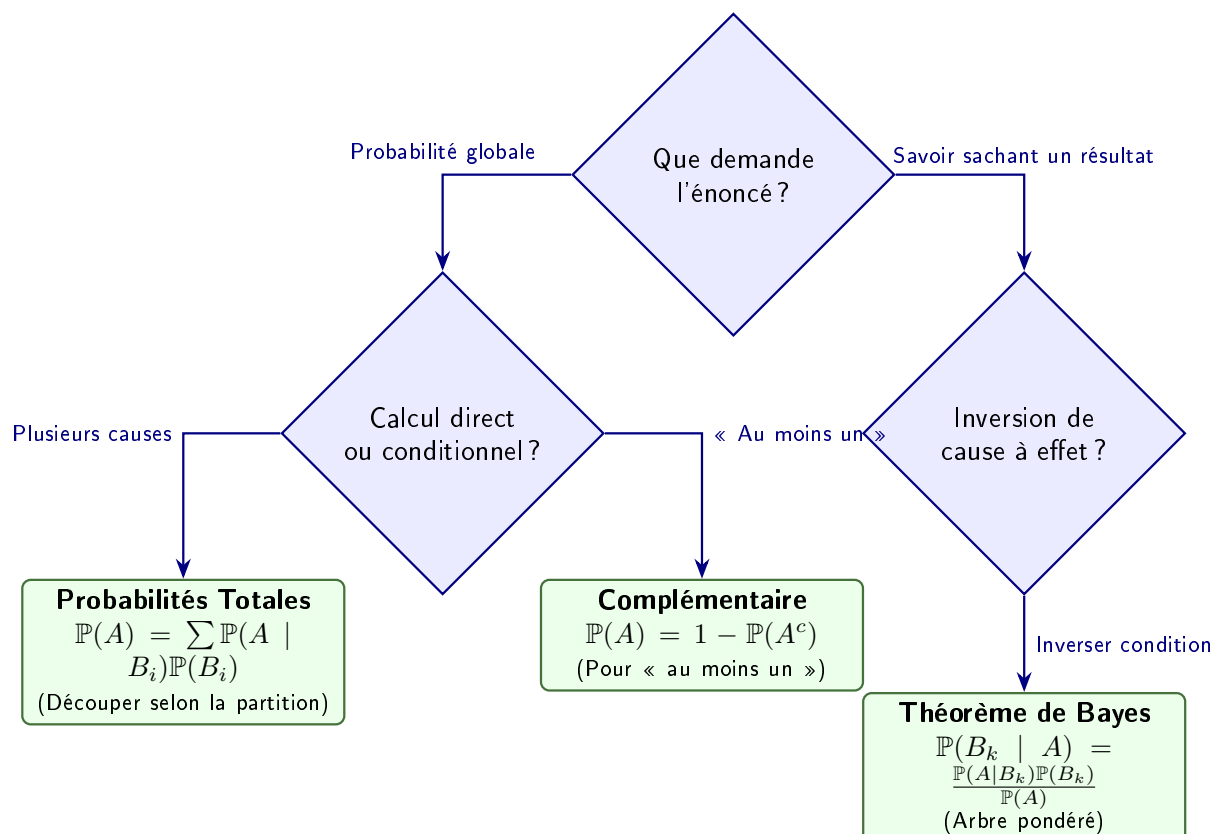
— Une famille $(A_i)_{i \in I}$ est **mutuellement indépendante** si pour tout sous-ensemble fini $J \subseteq I$:

$$\mathbb{P}\left(\bigcap_{j \in J} A_j\right) = \prod_{j \in J} \mathbb{P}(A_j)$$

— **Alerte :** L'indépendance 2 à 2 n'entraîne **pas** l'indépendance mutuelle !

4.2 Procédures de résolution

4.2.1 Arbre décisionnel : conditionnement et probabilités totales



4.2.2 Fiches de procédure opérationnelle

Procédure : Résolution Systématique d'un Problème Bayésien (Test Médical / Alarme)

Donnée : Un test ou diagnostic avec prévalence, sensibilité et spécificité.

Étape 1 Nommer clairement les événements :

- M : « L'individu est malade » (ou l'état vrai H_1). Prévalence : $\mathbb{P}(M)$.
- T : « Le test est positif ».

Étape 2 Identifier les données de l'énoncé :

- Sensibilité : $\mathbb{P}(T | M)$.
- Taux de faux négatif : $\mathbb{P}(T^c | M) = 1 - \mathbb{P}(T | M)$.
- Spécificité : $\mathbb{P}(T^c | M^c)$.
- Taux de faux positif : $\mathbb{P}(T | M^c) = 1 - \mathbb{P}(T^c | M^c)$.

Étape 3 Calcul du dénominateur (Probabilités totales) :

$$\mathbb{P}(T) = \mathbb{P}(T | M)\mathbb{P}(M) + \mathbb{P}(T | M^c)\mathbb{P}(M^c)$$

Étape 4 Application de la formule de Bayes :

$$\mathbb{P}(M | T) = \frac{\mathbb{P}(T | M)\mathbb{P}(M)}{\mathbb{P}(T)}$$

Procédure : Analyse au Premier Pas (First-Step Analysis) pour Processus Séquentiels

Donnée : Un jeu répété ou processus stochastique à étapes successives (ex : premier joueur à obtenir Pile, jeu interrompu, ruine du joueur).

Étape 1 Définir l'inconnue globale : Poser p la probabilité de victoire finale du joueur ciblé (ou h le nombre espéré d'étapes jusqu'à absorption).

Étape 2 Conditionner sur la première transition complète : Décomposer par la formule des probabilités totales selon les issues possibles du premier tour de jeu :

$$p = \mathbb{P}(\text{Victoire immédiate}) + \mathbb{P}(\text{Poursuite du jeu}) \times \mathbb{P}(\text{Gagner} | \text{Poursuite})$$

Étape 3 Exploiter l'invariance ou la symétrie temporelle : Par indépendance des tours successifs, $\mathbb{P}(\text{Gagner} | \text{Poursuite})$ se réexprime directement en fonction de p (ou de la probabilité de l'autre joueur $1 - p$).

Étape 4 Résoudre l'équation algébrique de point fixe : Isoler p .

- **Exemple type examen (Duel de pièces) :** Deux joueurs A et B lancent alternativement une pièce. A gagne si Face avec proba p_1 , sinon B lance avec proba p_2 . La probabilité que A gagne vérifie :

$$p_A = p_1 + (1 - p_1)(1 - p_2)p_A \implies p_A = \frac{p_1}{1 - (1 - p_1)(1 - p_2)}$$

Attention – Pièges classiques d'examen sur le Conditionnement

- **Sophisme du procureur :** Ne **jamais** confondre $\mathbb{P}(A | B)$ et $\mathbb{P}(B | A)$. Par exemple, la probabilité d'avoir un test positif sachant qu'on est malade ($\approx 99\%$) n'a RIEN À VOIR avec la probabilité d'être malade sachant que le test est positif (qui peut valoir $< 5\%$ si la maladie est rare!).
- **Disjoints $\neq$ Indépendants :** Deux événements disjoints non triviaux ($A \cap B = \emptyset$ avec $\mathbb{P}(A) > 0, \mathbb{P}(B) > 0$) vérifient $\mathbb{P}(A \cap B) = 0 \neq \mathbb{P}(A)\mathbb{P}(B)$. Ils ne sont donc **jamais indépendants** !

S'ils sont disjoints, savoir que B se produit garantit que A ne peut PAS se produire ($\mathbb{P}(A | B) = 0$).

Astuce – Raccourcis d'examen express

- **Arbre de probabilités annoté** : Pour tout exercice à étapes successives, dessiner un arbre à 2 niveaux. La probabilité d'une feuille est le produit des branches. $\mathbb{P}(A)$ est la somme des feuilles menant à A .
- **Mise à jour séquentielle de Bayes** : Si un individu effectue un second test T_2 indépendant conditionnellement à son état, la probabilité a posteriori $\mathbb{P}(M | T_1)$ devient le nouvel **a priori** pour le second test :

$$\mathbb{P}(M | T_1 \cap T_2) = \frac{\mathbb{P}(T_2 | M) \mathbb{P}(M | T_1)}{\mathbb{P}(T_2 | M) \mathbb{P}(M | T_1) + \mathbb{P}(T_2 | M^c) \mathbb{P}(M^c | T_1)}$$

- **Loi de succession de Laplace** : Après avoir observé k succès lors de n essais indépendants sous a priori uniforme, la probabilité que le prochain essai soit un succès est directement $\frac{k+1}{n+2}$.

4.2.3 Exemples résolus réels tirés des examens

Exemple – Examen Janvier 2024 : Test de dépistage et Paradoxe des Faux Positifs

Énoncé : Une maladie rare touche 0.1% de la population ($\mathbb{P}(M) = 0.001$). Un laboratoire conçoit un test de dépistage dont la sensibilité vaut 99% ($\mathbb{P}(T | M) = 0.99$) et le taux de faux positifs est de 2% ($\mathbb{P}(T | M^c) = 0.02$). Un patient effectue le test et obtient un résultat positif. Quelle est la probabilité réelle qu'il soit malade ?

Résolution pas-à-pas :

- Données : $\mathbb{P}(M) = 0.001 \implies \mathbb{P}(M^c) = 0.999$. $\mathbb{P}(T | M) = 0.99$, $\mathbb{P}(T | M^c) = 0.02$.
- Probabilité totale d'obtenir un test positif :

$$\begin{aligned} \mathbb{P}(T) &= \mathbb{P}(T | M) \mathbb{P}(M) + \mathbb{P}(T | M^c) \mathbb{P}(M^c) \\ &= (0.99 \times 0.001) + (0.02 \times 0.999) \\ &= 0.00099 + 0.01998 = 0.02097 \quad (\approx 2.1\%) \end{aligned}$$

- Inversion par Bayes :

$$\mathbb{P}(M | T) = \frac{\mathbb{P}(T | M) \mathbb{P}(M)}{\mathbb{P}(T)} = \frac{0.00099}{0.02097} \approx \boxed{0.0472 \quad (4.72\%)}$$

Interprétation d'examen : Malgré un test précis à 99%, un individu testé positif a moins de 5% de chance d'être malade, car les faux positifs issus de la population saine (99.9%) submergent largement les vrais positifs !

5 Variables Aléatoires & Lois Usuelles (Discrètes et Continues)

Une variable aléatoire est une fonction mesurable $X : \Omega \rightarrow \mathbb{R}$ associant un nombre à chaque issue du hasard. C'est l'outil par excellence de la modélisation en ingénierie. Ce chapitre compile de façon exhaustive les **7 lois maîtresses du formulaire officiel UCLouvain**, leurs espérances, variances et fonctions génératrices des moments, ainsi que les méthodes de calcul de probabilités via standardisation normale.

5.1 Rappels théoriques

Définition – Fonction de Répartition

La **fonction de répartition** d'une variable aléatoire X est définie pour tout $x \in \mathbb{R}$ par :

$$F_X(x) = \mathbb{P}(X \leq x)$$

Propriétés universelles :

- F_X est croissante et continue à droite en tout point.
- $\lim_{x \rightarrow -\infty} F_X(x) = 0$ et $\lim_{x \rightarrow +\infty} F_X(x) = 1$.
- $\mathbb{P}(a < X \leq b) = F_X(b) - F_X(a)$.

Définition – Variables Discrètes vs Variables Continues

- **Variable discrète** : prend ses valeurs dans un ensemble dénombrable $\{x_1, x_2, \dots\}$. Caractérisée par sa fonction de masse $p_X(x_k) = \mathbb{P}(X = x_k)$ avec $\sum_k p_X(x_k) = 1$.
- **Variable continue** : caractérisée par une **densité de probabilité** $f_X(x) \geq 0$ telle que :

$$F_X(x) = \int_{-\infty}^x f_X(t) dt \implies f_X(x) = F'_X(x) \quad \text{et} \quad \int_{-\infty}^{+\infty} f_X(x) dx = 1$$

Règle fondamentale : Pour une variable continue, la probabilité ponctuelle est toujours nulle : $\mathbb{P}(X = x_0) = 0$. Donc $\mathbb{P}(a \leq X \leq b) = \mathbb{P}(a < X < b)$.

5.1.1 Le Catalogue Officiel des 7 Lois du Formulaire UCLouvain

Théorème – Les 5 Lois Discrètes du Formulaire Officiel

1. Loi de Bernoulli $\mathcal{B}(p)$:

- $X \in \{0, 1\}$, $\mathbb{P}(X = 1) = p$, $\mathbb{P}(X = 0) = q = 1 - p$.
- $\mathbb{E}[X] = p$, $\text{Var}(X) = pq$, MGF : $M_X(t) = q + pe^t$.

2. Loi Binomiale $\mathcal{B}(n, p)$ (Somme de n Bernoulli i.i.d.) :

- $\mathbb{P}(X = k) = \binom{n}{k} p^k q^{n-k}$ pour $k \in \{0, 1, \dots, n\}$.
- $\mathbb{E}[X] = np$, $\text{Var}(X) = npq$, MGF : $M_X(t) = (q + pe^t)^n$.

3. Loi Géométrique $\mathcal{G}(p)$ (! Convention Officielle UCLouvain) :

- Compte le **nombre d'essais infructueux avant le premier succès** ($x \in \mathbb{N}$) :

$$\mathbb{P}(X = x) = q^x p \quad (x \in \mathbb{N}), \quad F_X(x) = 1 - q^{\lfloor x+1 \rfloor} \quad (x \geq 0)$$

- $\mathbb{E}[X] = \frac{q}{p}$, $\text{Var}(X) = \frac{q}{p^2}$, MGF : $M_X(t) = \frac{p}{1 - qe^t}$.
- **Absence de mémoire discrète** : $\mathbb{P}(X \geq s + t \mid X \geq s) = \mathbb{P}(X \geq t)$.

4. Loi de Poisson $\mathcal{P}(\mu)$ (Événements rares, comptage d'arrivées) :

- $\mathbb{P}(X = k) = \frac{\mu^k}{k!} e^{-\mu}$ pour $k \in \mathbb{N}$ (avec $\mu = \lambda T$).
- $\mathbb{E}[X] = \mu$, $\text{Var}(X) = \mu$, MGF : $M_X(t) = e^{\mu(e^t - 1)}$.
- **Approximation de la Binomiale** : Si $n \geq 30$ et $p \leq 0.05$, $\mathcal{B}(n, p) \approx \mathcal{P}(\mu = np)$.

5. Loi Hypergéométrique $\mathcal{H}(N, K, n)$ (Échantillonnage sans remise) :

- Compte le nombre de succès k dans un tirage simultané (sans remise) de taille n au sein d'une population N contenant K succès (proportion $p = K/N$) :

$$\mathbb{P}(X = k) = \frac{\binom{K}{k} \binom{N-K}{n-k}}{\binom{N}{n}} \quad (\max(0, n - (N - K)) \leq k \leq \min(n, K))$$

- $\mathbb{E}[X] = n \frac{K}{N} = np$.
- $\text{Var}(X) = np(1-p) \frac{N-n}{N-1}$ (le terme $\frac{N-n}{N-1} < 1$ est le facteur d'exhaustion finie).
- **Approximation Binomiale** : Si $N \rightarrow \infty$ avec $n/N \ll 1$, $\mathcal{H}(N, K, n) \approx \mathcal{B}(n, p = K/N)$.

Théorème – Les Lois Continues du Formulaire et Loi d'Erlang**1. Loi Uniforme Continue $\mathcal{U}(a, b)$:**

- Densité $f(x) = \frac{1}{b-a}$ sur $[a, b]$, $F(x) = \frac{x-a}{b-a}$.
- $\mathbb{E}[X] = \frac{a+b}{2}$, $\text{Var}(X) = \frac{(b-a)^2}{12}$, MGF : $M_X(t) = \frac{e^{bt} - e^{at}}{(b-a)t}$.

2. Loi Exponentielle $\mathcal{E}(\lambda)$ (Temps d'attente sans mémoire) :

- Densité $f(x) = \lambda e^{-\lambda x}$ pour $x \geq 0$, $F(x) = 1 - e^{-\lambda x}$.
- $\mathbb{E}[X] = \frac{1}{\lambda}$, $\text{Var}(X) = \frac{1}{\lambda^2}$, MGF : $M_X(t) = \frac{\lambda}{\lambda - t}$ ($t < \lambda$).
- **Absence de mémoire continue** : $\mathbb{P}(X > s + t \mid X > s) = \mathbb{P}(X > t) = e^{-\lambda t}$.

3. Loi d'Erlang / Gamma Erlang(k, λ) (Somme de k exponentielles i.i.d.) :

- Si $X_1, \dots, X_k \sim \mathcal{E}(\lambda)$ indépendantes, alors $S_k = \sum_{i=1}^k X_i \sim \text{Erlang}(k, \lambda)$:

$$f_{S_k}(x) = \frac{\lambda^k x^{k-1}}{(k-1)!} e^{-\lambda x} \quad (x \geq 0)$$

- $\mathbb{E}[S_k] = \frac{k}{\lambda}$, $\text{Var}(S_k) = \frac{k}{\lambda^2}$, MGF : $M_{S_k}(t) = \left(\frac{\lambda}{\lambda - t} \right)^k$ ($t < \lambda$).

4. Loi Normale (Gaussienne) $\mathcal{N}(\mu, \sigma^2)$:

- Densité $f(x) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right)$.
- $\mathbb{E}[X] = \mu$, $\text{Var}(X) = \sigma^2$, MGF : $M_X(t) = e^{\mu t + \sigma^2 t^2 / 2}$.
- **Standardisation** : $Z = \frac{X - \mu}{\sigma} \sim \mathcal{N}(0, 1)$.

Théorème – Changement de Variable Scalaire Continu (Formule de Transfert)

Soit X une variable aléatoire continue de densité $f_X(x)$ et $Y = g(X)$ où g est une fonction dérivable et strictement monotone (bijective) sur le support de X . La densité de probabilité de Y est donnée

par :

$$f_Y(y) = f_X(g^{-1}(y)) \cdot \left| \frac{d}{dy} g^{-1}(y) \right| = \frac{f_X(x)}{|g'(x)|} \quad \text{avec } x = g^{-1}(y)$$

Application type examen (Énergie cinétique) : Soit V une vitesse aléatoire positive de densité $f_V(v)$ et $E = \frac{1}{2}mV^2$. Comme $v = \sqrt{2E/m}$ et $\frac{dv}{dE} = \frac{1}{\sqrt{2mE}}$:

$$f_E(e) = f_V\left(\sqrt{\frac{2e}{m}}\right) \cdot \frac{1}{\sqrt{2me}} \quad (e > 0)$$

Définition – Couples de Variables Aléatoires Continues (Lois Bivariées)

Pour un couple (X, Y) de variables aléatoires continues de densité conjointe $f_{X,Y}(x, y) \geq 0$ vérifiant $\iint_{\mathbb{R}^2} f_{X,Y}(x, y) dx dy = 1$:

— **Densités marginales** : Obtenues par intégration sur la variable non observée :

$$f_X(x) = \int_{-\infty}^{+\infty} f_{X,Y}(x, y) dy \quad \text{et} \quad f_Y(y) = \int_{-\infty}^{+\infty} f_{X,Y}(x, y) dx$$

— **Densité conditionnelle** : $f_{Y|X}(y | x) = \frac{f_{X,Y}(x, y)}{f_X(x)}$ pour tout x tel que $f_X(x) > 0$.

— **Critère d'indépendance continue** : X et Y sont indépendantes si et seulement si pour tout (x, y) :

$$f_{X,Y}(x, y) = f_X(x) \cdot f_Y(y)$$

— **Calcul d'espérance bivariée** : $\mathbb{E}[g(X, Y)] = \iint_{\mathbb{R}^2} g(x, y) f_{X,Y}(x, y) dx dy$. En particulier :

$$\text{Cov}(X, Y) = \iint_{\mathbb{R}^2} (x - \mathbb{E}[X])(y - \mathbb{E}[Y]) f_{X,Y}(x, y) dx dy = \mathbb{E}[XY] - \mathbb{E}[X]\mathbb{E}[Y]$$

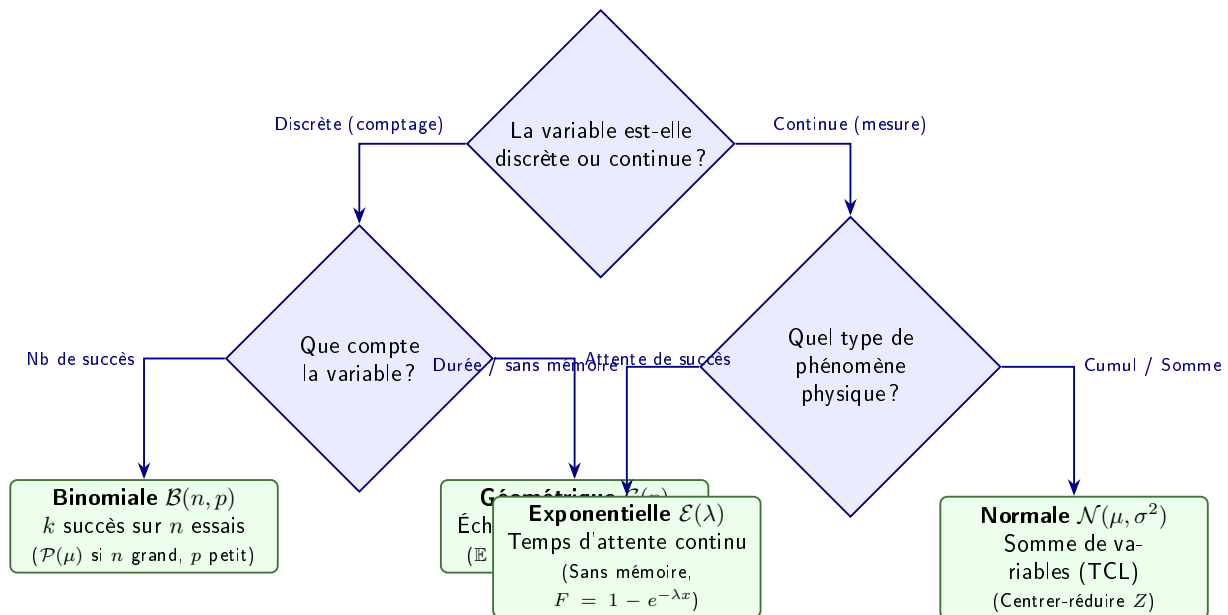
Propriété – Table Numérique Officielle de la Normale Centrée Réduite

Pour $Z \sim \mathcal{N}(0, 1)$, le formulaire officiel fournit rigoureusement les valeurs de $F(z) = \mathbb{P}(Z \leq z)$:

z	-3	-2	-1	0	1	2	3
$F(z)$	0.0013	0.0228	0.1587	0.5000	0.8413	0.9772	0.9987

Symétrie fondamentale : $F(-z) = 1 - F(z) \implies \mathbb{P}(Z > 2) = 1 - F(2) = 1 - 0.9772 = 0.0228 = 2.28\%$.

5.2.1 Arbre décisionnel : identification de la loi de probabilité



5.2.2 Fiches de procédure opérationnelle

Procédure : Calcul de Probabilité Normale par Standardisation

Donnée : Une variable $X \sim \mathcal{N}(\mu, \sigma^2)$ et un intervalle $[a, b]$.

Étape 1 Centrage et réduction : Définir $Z = \frac{X - \mu}{\sigma} \sim \mathcal{N}(0, 1)$.

Étape 2 Transformation des bornes :

$$z_a = \frac{a - \mu}{\sigma}, \quad z_b = \frac{b - \mu}{\sigma}$$

Étape 3 Expression avec la fonction de répartition F :

$$\mathbb{P}(a \leq X \leq b) = \mathbb{P}(z_a \leq Z \leq z_b) = F(z_b) - F(z_a)$$

Étape 4 Exploitation de la symétrie si $z < 0$: Utiliser $F(-z) = 1 - F(z)$.

Étape 5 Lecture dans la table du formulaire : Remplacer par les valeurs numériques officielles.

Attention – Pièges classiques d'examen sur les Loïs de Probabilités

- **Convention UCLouvain de la loi géométrique :** Dans d'autres universités, $\mathcal{G}(p)$ compte le rang du premier succès ($k \geq 1, \mathbb{E} = 1/p$). **À l'UCLouvain (formulaire officiel),** X compte le **nombre d'échecs avant le premier succès** ($x \in \mathbb{N}$), d'où :

$$\mathbb{E}[X] = \frac{q}{p} = \frac{1-p}{p}, \quad \text{Var}(X) = \frac{q}{p^2} = \frac{1-p}{p^2}$$

Si l'énoncé demande le nombre total d'essais $Y = X + 1$, penser à ajouter 1 à l'espérance !

- **Écart-type vs Variance :** Dans $\mathcal{N}(\mu, \sigma^2)$, le second paramètre est σ^2 (la variance). Lors de la standardisation, on divise par $\sigma = \sqrt{\text{Var}(X)}$ et JAMAIS par σ^2 !

Astuce – Raccourcis d'examen express

- **Superposition de Poisson** : Si $X_1 \sim \mathcal{P}(\lambda_1)$ et $X_2 \sim \mathcal{P}(\lambda_2)$ sont indépendantes, leur somme suit directement $X_1 + X_2 \sim \mathcal{P}(\lambda_1 + \lambda_2)$.
- **Minimum d'exponentielles indépendantes** : Si $T_1 \sim \mathcal{E}(\lambda_1)$ et $T_2 \sim \mathcal{E}(\lambda_2)$ sont indépendantes, le premier événement qui survient est $T_{\min} = \min(T_1, T_2) \sim \mathcal{E}(\lambda_1 + \lambda_2)$.

5.2.3 Exemples résolus réels tirés des examens**Exemple – Examen Janvier 2025, Question 2d : Approximation normale d'un saut de puce**

Énoncé : À chaque pas s , une puce avance de $Y_s \in \{1, 2\}$ avec probabilités $1/2$ et $1/2$. On note $X_s = \sum_{i=0}^{s-1} Y_i$ sa position à l'étape s . Pour $s = 10\,000$, la puce se trouve entre 10 000 et 20 000. Quelle est la probabilité que $15\,100 \leq X_{10\,000} \leq 20\,000$?

Résolution pas-à-pas :

- Pour un saut individuel Y : $\mathbb{E}[Y] = \frac{1}{2}(1) + \frac{1}{2}(2) = 1.5 = \frac{3}{2}$. $\mathbb{E}[Y^2] = \frac{1}{2}(1) + \frac{1}{2}(4) = 2.5 = \frac{5}{2} \implies \text{Var}(Y) = \frac{5}{2} - \left(\frac{3}{2}\right)^2 = \frac{1}{4}$.
- Pour $s = 10\,000$, X_s est la somme de 10 000 variables i.i.d. :

$$\mu = \mathbb{E}[X_s] = 10\,000 \times \frac{3}{2} = 15\,000, \quad \text{Var}(X_s) = 10\,000 \times \frac{1}{4} = 2\,500 \implies \sigma = \sqrt{2\,500} = 50$$

- Par le Théorème Central Limite ($s \gg 1$), $X_s \approx \mathcal{N}(\mu = 15\,000, \sigma^2 = 2\,500)$.
- Standardisation de la borne inférieure 15 100 :

$$z = \frac{15\,100 - 15\,000}{50} = \frac{100}{50} = 2$$

- Comme la borne supérieure 20 000 correspond à $z = \frac{5\,000}{50} = 100 \gg 3$ (probabilité 1), on a :

$$\mathbb{P}(15\,100 \leq X_s \leq 20\,000) \approx \mathbb{P}(Z \geq 2) = 1 - F(2)$$

- D'après la table numérique officielle du formulaire : $F(2) = 0.9772$.

$$\mathbb{P}(X_s \geq 15\,100) = 1 - 0.9772 = 0.0228 = \boxed{2.2\%}$$

6 Espérance, Variance & Théorèmes de Concentration

L'espérance et la variance résument le comportement moyen et l'incertitude d'un système stochastique. Lorsque la loi exacte d'une variable aléatoire est inaccessible ou trop lourde à expliciter, les **inégalités de concentration** (Markov, Bienaymé-Tchebychev, Chernoff) et le **Théorème Central Limite** (TCL) permettent d'obtenir des bornes strictes ou des approximations asymptotiques garanties.

6.1 Rappels théoriques

Définition – Espérance et Théorème du Transfert

- **Cas discret** : $\mathbb{E}[X] = \sum_k x_k \mathbb{P}(X = x_k)$. **Cas continu** : $\mathbb{E}[X] = \int_{-\infty}^{+\infty} x f_X(x) dx$.
- **Théorème du transfert** : Pour toute fonction réelle g :

$$\mathbb{E}[g(X)] = \sum_k g(x_k) \mathbb{P}(X = x_k) \quad \text{ou} \quad \int_{-\infty}^{+\infty} g(x) f_X(x) dx$$

Théorème – Propriété d'Or : Linéarité Inconditionnelle de l'Espérance

Pour toutes variables aléatoires $X_1, \dots, X_n$ (qu'elles soient **indépendantes** ou **dépendantes**) et toutes constantes $a_i \in \mathbb{R}$:

$$\mathbb{E} \left[\sum_{i=1}^n a_i X_i \right] = \sum_{i=1}^n a_i \mathbb{E}[X_i]$$

Méthode des variables indicatrices : Si $X = \sum_{i=1}^n \mathbf{1}_{A_i}$ compte le nombre d'événements réalisés parmi $A_1, \dots, A_n$, alors :

$$\mathbb{E}[X] = \sum_{i=1}^n \mathbb{P}(A_i)$$

même si les A_i sont fortement corrélés !

Définition – Variance, Covariance et Corrélation

- **Variance** : $\text{Var}(X) = \mathbb{E}[(X - \mathbb{E}[X])^2] = \mathbb{E}[X^2] - (\mathbb{E}[X])^2 \geq 0$.
- **Écart-type** : $\sigma(X) = \sqrt{\text{Var}(X)}$. Homogénéité : $\text{Var}(aX + b) = a^2 \text{Var}(X)$.
- **Covariance** : $\text{Cov}(X, Y) = \mathbb{E}[XY] - \mathbb{E}[X]\mathbb{E}[Y]$.
- **Variance d'une somme générale** :

$$\text{Var} \left(\sum_{i=1}^n X_i \right) = \sum_{i=1}^n \text{Var}(X_i) + 2 \sum_{1 \leq i < j \leq n} \text{Cov}(X_i, X_j)$$

Si les X_i sont deux à deux non corrélés (en particulier s'ils sont indépendants) : $\text{Var}(\sum X_i) = \sum \text{Var}(X_i)$.

Théorème – Inégalités de Concentration (Formulaire Officiel)

Pour une variable aléatoire réelle quelconque :

1. **Inégalité de Markov** : Si X est une variable positive ($X \geq 0$), alors pour tout $a > 0$:

$$\mathbb{P}(X \geq a\mathbb{E}[X]) \leq \frac{1}{a} \iff \mathbb{P}(X \geq c) \leq \frac{\mathbb{E}[X]}{c} \quad (c > 0)$$

2. Inégalité de Bienaymé-Tchebychev : Pour tout $a > 0$:

$$\mathbb{P}(|X - \mathbb{E}[X]| \geq a\sigma(X)) \leq \frac{1}{a^2} \iff \mathbb{P}(|X - \mu| \geq \varepsilon) \leq \frac{\text{Var}(X)}{\varepsilon^2}$$

3. Inégalité de Chernoff : Pour tout $x \in \mathbb{R}$ et pour tout $t > 0$:

$$\mathbb{P}(X \geq x) \leq e^{-tx} \mathbb{E}[e^{tX}]$$

Théorème – Loi des Grands Nombres et Théorème Central Limite (TCL)

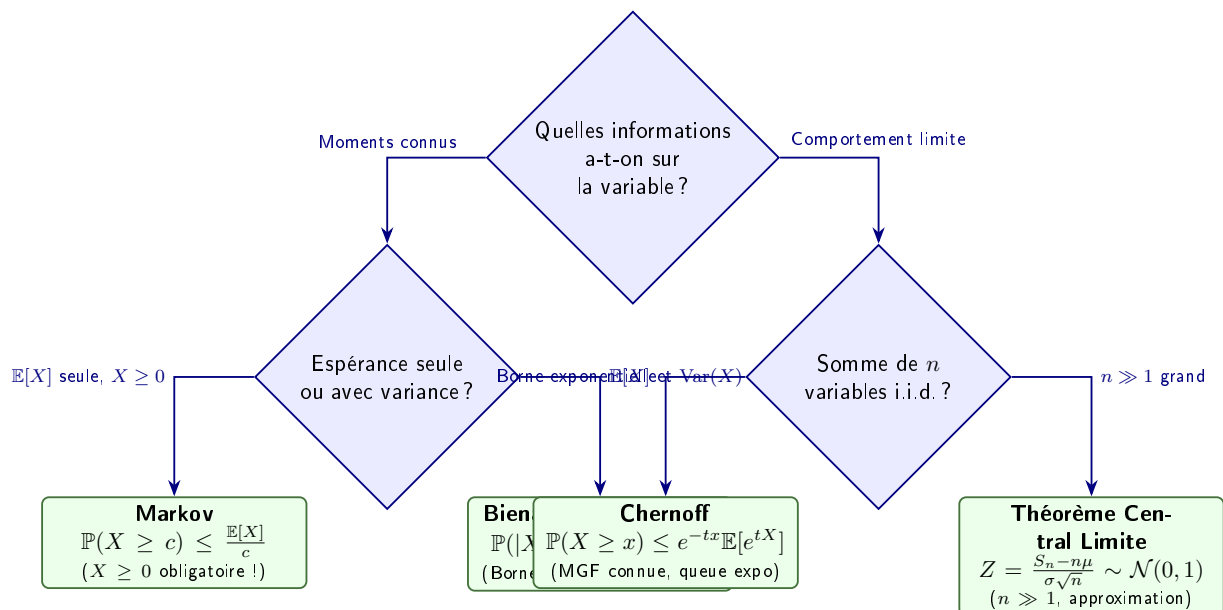
Soient $X_1, \dots, X_n$ des variables indépendantes et identiquement distribuées (i.i.d.) d'espérance μ et d'écart-type σ . Soit $S_n = \sum_{i=1}^n X_i$ et $\bar{X}_n = \frac{S_n}{n}$.

- **Loi Faible des Grands Nombres (LLN) :** $\forall \varepsilon > 0, \lim_{n \rightarrow \infty} \mathbb{P}(|\bar{X}_n - \mu| \geq \varepsilon) = 0$.
- **Théorème Central Limite (TCL) :** Lorsque $n \rightarrow \infty$, la somme normalisée converge en loi vers la normale :

$$Z_n = \frac{S_n - n\mu}{\sigma\sqrt{n}} = \frac{\bar{X}_n - \mu}{\sigma/\sqrt{n}} \xrightarrow{\mathcal{D}} \mathcal{N}(0, 1)$$

6.2 Procédures de résolution

6.2.1 Arbre décisionnel : quelle inégalité ou théorème utiliser ?



6.2.2 Fiches de procédure opérationnelle

Procédure : Calcul d'Espérance Complexe par Variables Indicatrices

Donnée : Un décompte X du nombre d'éléments satisfaisant une propriété (ex : nombre de points fixes, nombre de paires appariées, nombre de sommets isolés).

Étape 1 Décomposition en indicatrices : Écrire $X = \sum_{i=1}^n I_i$ où $I_i = \mathbf{1}_{A_i} \in \{0, 1\}$ vaut 1 si le i -ème objet satisfait la condition et 0 sinon.

Étape 2 Calcul de la probabilité individuelle : Déterminer $\mathbb{P}(A_i)$. En général, par symétrie, tous les $\mathbb{P}(A_i)$ sont identiques : $\mathbb{P}(A_i) = p$.

Étape 3 Application de la linéarité :

$$\mathbb{E}[X] = \mathbb{E}\left[\sum_{i=1}^n I_i\right] = \sum_{i=1}^n \mathbb{E}[I_i] = \sum_{i=1}^n \mathbb{P}(A_i) = n \cdot p$$

Rappel crucial : Aucune hypothèse d'indépendance n'est requise !

Attention – Pièges classiques d'examen sur les Théorèmes de Concentration

- **Décorrélation $\neq$ Indépendance (Le piège d'examen n°1) :** X et Y indépendantes $\implies \text{Cov}(X, Y) = 0$. Mais la réciproque est **FAUSSE** en général !
 - **Contre-exemple canonique du recueil :** Soit X symétrique sur $[-1, 1]$ (ex : uniforme ou $\mathbb{P}(X = \pm 1) = \mathbb{P}(X = 0) = 1/3$) et $Y = X^2$. On a $\mathbb{E}[X] = 0$ et $\mathbb{E}[XY] = \mathbb{E}[X^3] = 0$, donc $\text{Cov}(X, Y) = 0$ (corrélation nulle). Pourtant, Y est **strictement déterminée par** X (dépendance fonctionnelle absolue) !
 - **Seule exception :** La réciproque n'est vraie que si le couple (X, Y) est **conjointement gaussien** (vecteur normal).
- **Hypothèse de positivité pour Markov :** L'inégalité de Markov $\mathbb{P}(X \geq c) \leq \frac{\mathbb{E}[X]}{c}$ est **strictement fautive** si X peut prendre des valeurs négatives ! Si X n'est pas positive, passer à Tchebychev ou poser $Y = X - \min(X)$.
- **Sens de l'inégalité de Tchebychev :** Tchebychev borne une probabilité de **dévi**ation (au-delà de ε). Si l'énoncé demande la probabilité d'être **proche** de la moyenne ($|X - \mu| \leq \varepsilon$), prendre le complémentaire :

$$\mathbb{P}(|X - \mu| \leq \varepsilon) = 1 - \mathbb{P}(|X - \mu| > \varepsilon) \geq 1 - \frac{\sigma^2}{\varepsilon^2}$$

Astuce – Raccourcis d'examen express

- **Coupon Collector's Problem (Temps d'attente complet) :** Pour obtenir n vignettes distinctes par tirages uniformes avec remise, le temps d'attente total $T = \sum_{i=1}^n T_i$ (où $T_i \sim \mathcal{G}(\frac{n-i+1}{n})$) vérifie :

$$\mathbb{E}[T] = nH_n = n \sum_{k=1}^n \frac{1}{k} \approx n \ln n + \gamma n, \quad \text{Var}(T) \leq \frac{\pi^2}{6} n^2$$

- **Paradoxe des Anniversaires :** Dans un groupe de n personnes sur $N = 365$ jours :

$$\mathbb{P}(\geq 1 \text{ collision}) = 1 - \frac{A_N^n}{N^n} \geq 50\% \quad \text{dès } n \geq 23, \quad \mathbb{E}[\text{paires identiques}] = \binom{n}{2} \frac{1}{N}$$

- **Comparaison immédiate des bornes :** Pour une même déviation, la précision des bornes suit toujours : Markov (très lâche) $\leq$ Tchebychev (bonne) $\leq$ Chernoff (exponentiellement précise) $\leq$ TCL (approximation normale exacte).
- **Variance d'indicatrices :** Pour $I = \mathbf{1}_A$, $\text{Var}(I) = p(1 - p)$ où $p = \mathbb{P}(A)$.

6.2.3 Exemples résolus réels tirés des examens**Exemple – Examen Janvier 2023 : Comparaison Markov vs Tchebychev**

Énoncé : Soit X le nombre de faces obtenues lors de 100 lancers d'une pièce équilibrée ($X \sim \mathcal{B}(100, 0.5)$). On sait que $\mathbb{E}[X] = 50$ et $\text{Var}(X) = 100 \times 0.5 \times 0.5 = 25$ ($\sigma = 5$). Borner la probabilité que $X \geq 75$.

Résolution pas-à-pas :

— **Borne de Markov** : Comme $X \geq 0$:

$$\mathbb{P}(X \geq 75) \leq \frac{\mathbb{E}[X]}{75} = \frac{50}{75} = \frac{2}{3} \approx 0.6667$$

— **Borne de Bienaymé-Tchebychev** : Remarquons que $X \geq 75 \implies |X - 50| \geq 25$. Dès lors :

$$\mathbb{P}(X \geq 75) \leq \mathbb{P}(|X - 50| \geq 25) \leq \frac{\text{Var}(X)}{25^2} = \frac{25}{625} = \frac{1}{25} = \boxed{0.04}$$

— **Approximation par le TCL** : $Z = \frac{75-50}{5} = \frac{25}{5} = 5$. D'après la loi normale, $\mathbb{P}(Z \geq 5) \approx 2.87 \times 10^{-7}$.

On constate de façon saisissante le gain de précision en exploitant la variance (Tchebychev donne 4% contre 66.7% pour Markov).

7 Fonctions Génératrices & Applications Stochastiques

Les fonctions génératrices transforment des opérations discrètes complexes (convolutions de suites, récurrences linéaires, sommes de variables aléatoires indépendantes) en de simples multiplications ou dérivations de polynômes et fractions rationnelles. Ce chapitre couvre les séries génératrices ordinaires (OGF), les fonctions génératrices des moments (MGF), ainsi que les chaînes de Markov et l'algorithme PageRank de Google.

7.1 Rappels théoriques

Définition – Fonction Génératrice Ordinaire (OGF)

La **fonction génératrice ordinaire** d'une suite réelle $(a_n)_{n \geq 0}$ est la série formelle :

$$G(s) = \sum_{n=0}^{\infty} a_n s^n$$

Le coefficient a_n s'extrait par $[s^n]G(s) = \frac{1}{n!}G^{(n)}(0)$.

Propriété – Dictionnaire des Opérations sur les OGF

Opération sur la suite	Terme général	Fonction génératrice
Combinaison linéaire	$\alpha a_n + \beta b_n$	$\alpha A(s) + \beta B(s)$
Décalage à droite (retard)	a_{n-1} (avec $a_{-1} = 0$)	$sA(s)$
Décalage à gauche (avance)	a_{n+1}	$\frac{A(s) - a_0}{s}$
Multiplication par n	$n \cdot a_n$	$sA'(s)$
Convolution de Cauchy	$c_n = \sum_{k=0}^n a_k b_{n-k}$	$A(s) \cdot B(s)$
Somme cumulative	$S_n = \sum_{k=0}^n a_k$	$\frac{A(s)}{1-s}$

Séries fondamentales à connaître par cœur :

$$\frac{1}{1-s} = \sum_{n=0}^{\infty} s^n, \quad \frac{1}{1-as} = \sum_{n=0}^{\infty} a^n s^n, \quad \frac{1}{(1-s)^2} = \sum_{n=0}^{\infty} (n+1)s^n$$

Propriété – Résolution Directe des Récurrences Linéaires d'Ordre 2 (Équation Caractéristique)

Pour résoudre une récurrence linéaire homogène à coefficients constants $a_n = c_1 a_{n-1} + c_2 a_{n-2}$ ($c_2 \neq 0$) sans passer par les séries entières, on résout l'**équation caractéristique** associée :

$$r^2 - c_1 r - c_2 = 0 \quad \text{de discriminant } \Delta = c_1^2 + 4c_2$$

Racines de l'équation	Forme générale du terme a_n	Détermination
$\Delta > 0$: 2 racines réelles $r_1 \neq r_2$	$a_n = C_1 r_1^n + C_2 r_2^n$	C_1, C_2 via a_0, a_1
$\Delta = 0$: 1 racine réelle double r_0	$a_n = (C_1 + C_2 n) r_0^n$	C_1, C_2 via a_0, a_1
$\Delta < 0$: 2 racines complexes $r e^{\pm i\theta}$	$a_n = r^n (C_1 \cos(n\theta) + C_2 \sin(n\theta))$	$r = \sqrt{-c_2}$, $\cos \theta = \frac{c_1}{2\sqrt{-c_2}}$

Définition – Fonction Génératrice des Probabilités (PGF)

Pour une variable aléatoire discrète X à valeurs dans $\mathbb{N}$:

$$G_X(s) = \mathbb{E}[s^X] = \sum_{k=0}^{\infty} \mathbb{P}(X = k) s^k$$

Propriétés fondamentales :

- **Normalisation** : $G_X(1) = \sum_{k=0}^{\infty} \mathbb{P}(X = k) = 1$.
- **Calcul des moments par dérivation en $s = 1$** :

$$\mathbb{E}[X] = G'_X(1), \quad \mathbb{E}[X(X-1)] = G''_X(1) \implies \text{Var}(X) = G''_X(1) + G'_X(1) - (G'_X(1))^2$$

- **Somme de variables indépendantes** : Si X et Y sont indépendantes :

$$G_{X+Y}(s) = G_X(s) \cdot G_Y(s)$$

Définition – Chaînes de Markov Discrètes et Distribution Stationnaire

Un processus stochastique $(X_t)_{t \geq 0}$ sur un ensemble fini d'états $\{1, \dots, N\}$ est une **chaîne de Markov** s'il vérifie la propriété sans mémoire : $\mathbb{P}(X_{t+1} = j \mid X_t = i, \dots, X_0 = i_0) = \mathbb{P}(X_{t+1} = j \mid X_t = i) =: P_{ij}$.

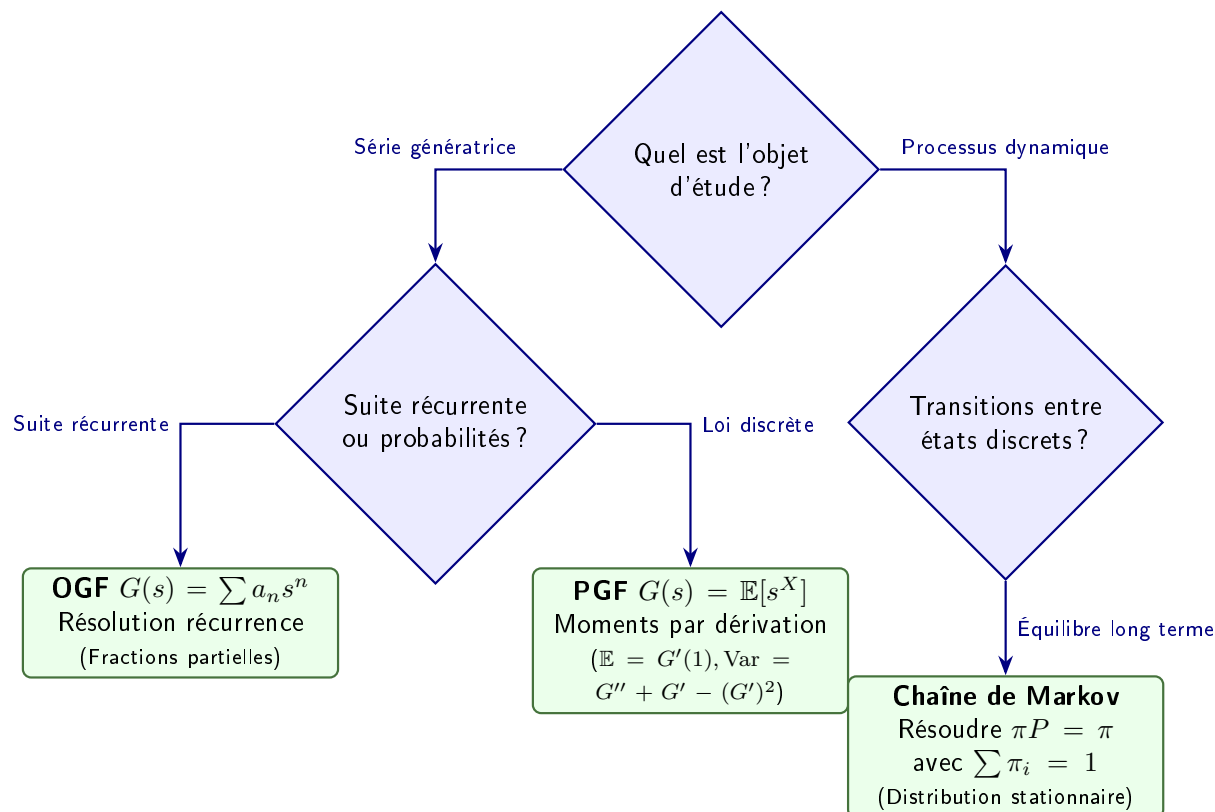
- **Matrice de transition P** : stochastique par ligne ($P_{ij} \geq 0$ et $\sum_{j=1}^N P_{ij} = 1$).
- **Distribution stationnaire π** : vecteur ligne $\pi = (\pi_1, \dots, \pi_N)$ vérifiant :

$$\pi P = \pi \quad \text{avec} \quad \sum_{i=1}^N \pi_i = 1 \quad \text{et} \quad \pi_i \geq 0$$

- **PageRank de Google** : Pour garantir l'irréductibilité et l'apériodicité sur le web, Google utilise la matrice de téléportation aléatoire avec facteur d'amortissement $\alpha \approx 0.85$:

$$G = \alpha P + \frac{1-\alpha}{N} \mathbf{1}\mathbf{1}^T$$

7.2.1 Arbre décisionnel : méthode de résolution stochastique



7.2.2 Fiches de procédure opérationnelle

Procédure : Résolution d'une Récurrence Linéaire par Fonction Génératrice

Donnée : Une relation de récurrence $a_n = c_1 a_{n-1} + c_2 a_{n-2} + f(n)$ pour $n \geq 2$, avec conditions initiales a_0, a_1 .

Étape 1 Multiplier par s^n et sommer pour $n \geq 2$:

$$\sum_{n=2}^{\infty} a_n s^n = c_1 s \sum_{n=2}^{\infty} a_{n-1} s^{n-1} + c_2 s^2 \sum_{n=2}^{\infty} a_{n-2} s^{n-2} + \sum_{n=2}^{\infty} f(n) s^n$$

Étape 2 Exprimer en fonction de $G(s) = \sum_{n=0}^{\infty} a_n s^n$:

$$G(s) - a_0 - a_1 s = c_1 s(G(s) - a_0) + c_2 s^2 G(s) + F(s)$$

Étape 3 Isoler algébriquement $G(s)$: Obtenir $G(s) = \frac{P(s)}{Q(s)}$.

Étape 4 Décomposition en éléments simples : Factoriser le dénominateur $Q(s)$ et décomposer en fractions partielles $\sum \frac{A_i}{1-r_i s}$.

Étape 5 Développement en série et identification : Utiliser $\frac{1}{1-r_i s} = \sum_{n=0}^{\infty} r_i^n s^n$ pour extraire la formule fermée :

$$a_n = [s^n]G(s) = \sum A_i r_i^n$$

Procédure : Calcul de la Distribution Stationnaire d'une Chaîne de Markov

Donnée : Une matrice de transition stochastique $P \in \mathbb{R}^{N \times N}$.

Étape 1 Poser le système d'équations : Écrire le produit ligne-matrice $\pi P = \pi$, c'est-à-dire :

$$\pi_j = \sum_{i=1}^N \pi_i P_{ij} \quad \text{pour tout } j \in \{1, \dots, N\}$$

Étape 2 Remplacer une équation redondante : Le système $\pi(P - I) = 0$ admet une infinité de solutions. Remplacer impérativement une des équations par la **condition de normalisation** :

$$\sum_{i=1}^N \pi_i = 1$$

Étape 3 Résoudre le système linéaire : Trouver l'unique solution respectant $\pi_i \geq 0$.

Procédure : Vérification Probabiliste Rapide de Produit Matriciel (Algorithme de Freivalds)

Donnée : Trois matrices carrées $A, B, C \in \mathbb{R}^{n \times n}$. On souhaite vérifier formellement si $A \cdot B = C$ en évitant le calcul du produit AB (qui coûte $\mathcal{O}(n^3)$ par méthode standard).

Étape 1 Tirage d'un vecteur binaire aléatoire : Générer un vecteur aléatoire $r = (r_1, \dots, r_n)^T \in \{0, 1\}^n$ où chaque composante r_i vaut 0 ou 1 avec probabilité 1/2 indépendamment.

Étape 2 Calcul associatif par produits matrice-vecteur en $\mathcal{O}(n^2)$:

- Calculer le vecteur $x = B \cdot r \in \mathbb{R}^n$ (coût n^2 opérations).
- Calculer le vecteur $y = A \cdot x = A(Br) \in \mathbb{R}^n$ (coût n^2 opérations).
- Calculer le vecteur $z = C \cdot r \in \mathbb{R}^n$ (coût n^2 opérations).

Attention capitale : Ne JAMAIS multiplier A par B ! Tout le gain algorithmique repose sur l'associativité $A(Br)$.

Étape 3 Test de conformité :

- Si $y \neq z$, alors $AB \neq C$ avec **certitude absolue** (100% de certitude, aucun faux négatif).
- Si $y = z$, on déclare que $AB = C$. La probabilité de faux positif (erreur) vérifie $\mathbb{P}(\text{erreur}) \leq \frac{1}{2}$.

Étape 4 Amplification par répétitions indépendantes : En répétant le test avec k vecteurs aléatoires indépendants $r^{(1)}, \dots, r^{(k)}$, si tous les tests donnent $A(Br) = Cr$, l'erreur résiduelle est bornée par :

$$\mathbb{P}(\text{Erreur après } k \text{ essais}) \leq \left(\frac{1}{2}\right)^k = 2^{-k}$$

Pour $k = 20$, la probabilité d'erreur devient inférieure à 10^{-6} en un temps total de seulement $\mathcal{O}(k \cdot n^2) \ll \mathcal{O}(n^3)$.

Attention – Pièges classiques d'examen sur les Fonctions Génératrices et Markov

- **Oubli des conditions initiales dans la sommation :** Lorsqu'on somme à partir de $n = 1$ ou $n = 2$, il faut **rigoureusement soustraire** a_0 ou $a_0 + a_1 s$ du terme de gauche !
- **Vecteur propre gauche vs droit :** La distribution stationnaire π est un vecteur propre **gauche** associé à la valeur propre 1 ($\pi P = \pi$). Résoudre $Pv = v$ donne un vecteur colonne constant $v = (1, \dots, 1)^T$, ce qui est inutile !

Astuce – Raccourcis d'examen express

- **Chaîne à deux états en 5 secondes** : Pour la matrice $P = \begin{pmatrix} 1-\alpha & \alpha \\ \beta & 1-\beta \end{pmatrix}$, la distribution stationnaire est directement :

$$\pi_1 = \frac{\beta}{\alpha + \beta}, \quad \pi_2 = \frac{\alpha}{\alpha + \beta}$$

- **Formule express pour PGF** : Si $G_X(s)$ est connue, calculer directement $G'_X(1)$ pour $\mathbb{E}[X]$ et $G''_X(1) + G'_X(1) - (G'_X(1))^2$ pour $\text{Var}(X)$ sans jamais développer la série.

7.2.3 Exemples résolus réels tirés des examens**Exemple – Examen Janvier 2025, Question 2f-g : Résolution par Fonction Génératrice**

Énoncé : La probabilité p_n que la puce aléatoire visite la position n vérifie la relation de récurrence suivante :

$$p_n + \frac{1}{2}p_{n-1} = 1 \quad \text{pour } n \geq 1, \quad \text{avec } p_0 = 1$$

Résoudre cette récurrence par la méthode de la fonction génératrice $f(s) = \sum_{n=0}^{\infty} p_n s^n$.

Résolution pas-à-pas intégrale :

- Multiplions la récurrence par s^n et sommons pour $n \geq 1$:

$$\sum_{n=1}^{\infty} p_n s^n + \frac{s}{2} \sum_{n=1}^{\infty} p_{n-1} s^{n-1} = \sum_{n=1}^{\infty} s^n$$

- En exprimant chaque terme via $f(s)$ et la série géométrique $\sum_{n=1}^{\infty} s^n = \frac{s}{1-s}$:

$$(f(s) - p_0) + \frac{s}{2}f(s) = \frac{s}{1-s} = \frac{1}{1-s} - 1$$

- Comme $p_0 = 1$, les -1 se simplifient de part et d'autre :

$$f(s) \left(1 + \frac{s}{2}\right) = \frac{1}{1-s} \implies f(s) = \frac{1}{(1-s)(1+s/2)}$$

- Décomposition en éléments simples : Cherchons A et B tels que :

$$\frac{1}{(1-s)(1+s/2)} = \frac{A}{1-s} + \frac{B}{1+s/2}$$

En multipliant par $(1-s)$ et en posant $s = 1$: $A = \frac{1}{1+1/2} = \frac{2}{3}$.

En multipliant par $(1+s/2)$ et en posant $s = -2$: $B = \frac{1}{1-(-2)} = \frac{1}{3}$.

- Réécriture de la série génératrice :

$$f(s) = \frac{2/3}{1-s} + \frac{1/3}{1-(-s/2)} = \frac{2}{3} \sum_{n=0}^{\infty} s^n + \frac{1}{3} \sum_{n=0}^{\infty} \left(-\frac{1}{2}\right)^n s^n$$

- Extraction du terme général $p_n = [s^n]f(s)$:

$$p_n = \frac{2}{3} + \frac{1}{3} \left(-\frac{1}{2}\right)^n$$

Vérification immédiate : $p_0 = \frac{2}{3} + \frac{1}{3} = 1$, $p_1 = \frac{2}{3} - \frac{1}{6} = \frac{1}{2}$, $p_2 = \frac{2}{3} + \frac{1}{12} = \frac{3}{4}$, parfaitement conforme !

8 Méthodes transversales & Réflexes d'examen

Ce dernier chapitre ne contient aucune nouvelle théorie, mais compile les **réflexes de survie opérationnels** et la grille de diagnostic transversal indispensables pour sécuriser le 20/20 le jour de l'épreuve.

8.1 Les *Red Flags* : signes que vous êtes sur la mauvaise piste

Si vous vous retrouvez dans l'une des situations suivantes pendant l'examen, **arrêtez-vous immédiatement** et appliquez l'alternative recommandée !

Attention – Red Flag 1 : Une combinatoire qui explose en 8 sous-cas inextricables

Situation d'alerte : Vous essayez de compter une distribution ou une sélection en découpant le problème en dizaines de cas particuliers en fonction des places ou des éléments manquants.

Que faire immédiatement ?

- **Passer au complémentaire :** Calculez $N_{\text{total}} - N_{\text{interdit}}$. Dès qu'un énoncé contient « au moins un » ou « au plus $n - 1$ », l'opposé s'exprime en une seule ligne.
- **Inclusion-Exclusion :** Si les interdictions se recoupent, écrivez formellement la formule d'inclusion-exclusion.
- **Étoiles et Barres :** Si les objets sont identiques, utilisez $\binom{n+k-1}{k}$ avec des variables décalées.

Attention – Red Flag 2 : Un calcul d'espérance bloqué sur une série infinie monstrueuse

Situation d'alerte : Vous cherchez la loi exacte $\mathbb{P}(X = k)$ d'un décompte aléatoire complexe pour en déduire $\mathbb{E}[X] = \sum k\mathbb{P}(X = k)$ et vous vous noyez dans les factorielles.

Que faire immédiatement ?

- **Variables indicatrices :** Décomposez impérativement $X = \sum I_i$ où $I_i = \mathbf{1}_{A_i}$. L'espérance est la somme des probabilités individuelles $\sum \mathbb{P}(A_i)$ **sans se soucier de l'indépendance**.
- **Fonction génératrice :** Si c'est une récurrence, écrivez l'OGF et calculez $G'(1)$.

Attention – Red Flag 3 : Dijkstra bloqué par un cycle ou un coût qui diminue indéfiniment

Situation d'alerte : Vous appliquez Dijkstra et vous constatez qu'une distance provisoire déjà validée devrait diminuer, ou que des arêtes ont des poids négatifs.

Que faire immédiatement ?

- **Arrêter Dijkstra :** Dijkstra ne fonctionne pas avec des poids négatifs.
- **Basculer sur Bellman-Ford** ou, si le graphe est acyclique (DAG), trier topologiquement les sommets pour relaxer en $\mathcal{O}(|V| + |E|)$.

Attention – Red Flag 4 : Une probabilité calculée > 1 ou < 0

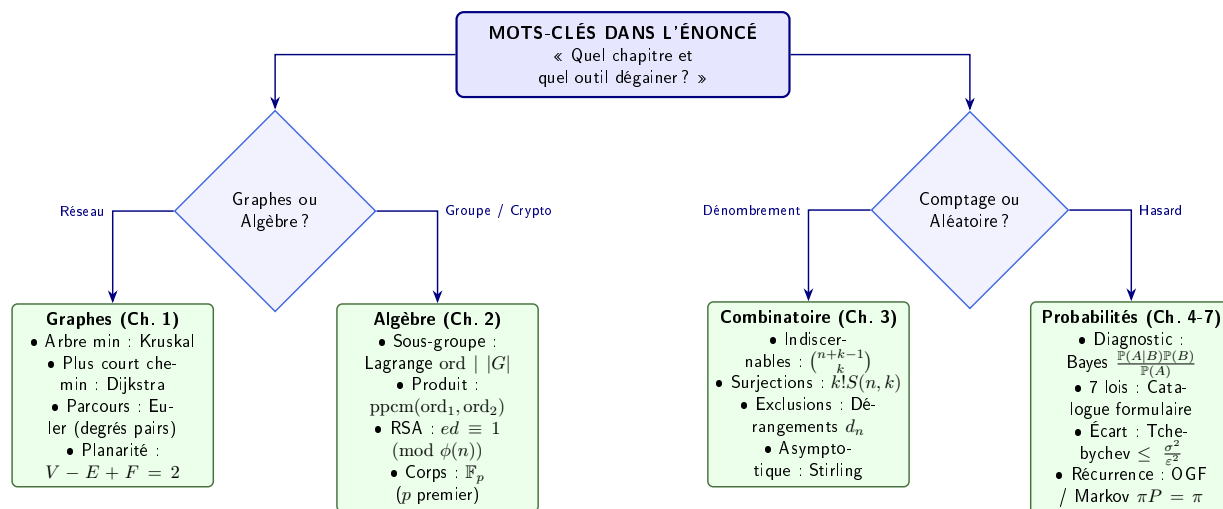
Situation d'alerte : Le résultat d'un calcul de probabilités ou d'un terme de Bayes donne une valeur négative ou strictement supérieure à 1.

Que faire immédiatement ?

- Vous avez confondu une union non disjointe ($\mathbb{P}(A \cup B) \neq \mathbb{P}(A) + \mathbb{P}(B)$ sans soustraire $\mathbb{P}(A \cap B)$).
- Dans Bayes, vous avez inversé le numérateur : le terme conditionnel direct est $\mathbb{P}(\text{Test} \mid \text{Malade})$ et non l'inverse.

8.2 L'Arbre Décisionnel Ultime Transversal

Ce schéma aiguille instantanément l'énoncé d'examen vers l'outil optimal :



8.3 Vérifications de bon sens (Sanity Checks)

Prenez 20 secondes à la fin de chaque question d'examen pour vérifier ces 8 règles d'or :

- Cohérence absolue des probabilités** : Une probabilité est **strictement comprise entre 0 et 1**. Une espérance de variable positive est positive ($\mathbb{E}[X] \geq 0$). Une variance est **toujours strictement positive ou nulle** ($\text{Var}(X) \geq 0$). Si votre variance est négative, vous avez inversé les termes dans $\mathbb{E}[X^2] - (\mathbb{E}[X])^2$.
- Parité des degrés d'un graphe** : La somme des degrés de tous les sommets est obligatoirement un nombre **pair** égal à $2|E|$. S'il y a un nombre impair de sommets de degré impair, recomptez immédiatement.
- Comptage des arêtes d'un arbre ou d'une forêt** : Tout arbre sous-tendant ou arbre à n sommets contient **exactement** $n - 1$ **arêtes**. Une forêt à n sommets et c composantes connexes contient exactement $n - c$ **arêtes**.
- Bipartisme et cycles impairs** : Un graphe biparti ne peut contenir **aucun cycle de longueur impaire** (aucun triangle C_3 , aucun pentagone C_5). Si votre graphe contient ne serait-ce qu'un triangle, il n'est **jamais biparti**.
- Divisibilité de Lagrange** : L'ordre calculé d'un sous-groupe ou d'un élément doit **impérativement diviser** l'ordre total du groupe. Dans $\mathbb{Z}_5 \times \mathbb{Z}_8$ ($|G| = 40$), un ordre de 7 est rigoureusement impossible. Dans $\mathbb{Z}_p^*$, tout ordre divise $p - 1$.
- Normalisation d'une chaîne de Markov** : La somme des probabilités de chaque ligne d'une matrice de transition vaut 1. La somme des composantes de la distribution stationnaire vaut **strictement 1** ($\sum_{i=1}^N \pi_i = 1$) avec $\pi_i \geq 0$.
- Décorrélation $\not\Rightarrow$ Indépendance** : Ne concluez **jamais** que deux variables sont indépendantes au seul motif que $\text{Cov}(X, Y) = 0$ (sauf s'il est explicitement précisé que le couple est conjointement gaussien).
- Bornes physiques de l'hypergéométrie** : Dans une loi hypergéométrique $\mathcal{H}(N, K, n)$, le nombre de succès k ne peut en aucun cas dépasser la taille de l'échantillon n , ni le stock de succès disponibles K : $\max(0, n - (N - K)) \leq k \leq \min(n, K)$.