Mathématiques Discrètes

Notes de Cours

Licence L2 — 2025–2026

Yaë Ulrich Gaba

« Dieu a fait les nombres entiers ; tout le reste est l'œuvre de l'homme. »

— Leopold Kronecker

25 mars 2026

Préface

Les **mathématiques discrètes** constituent le socle théorique sur lequel repose une grande partie de l'informatique moderne. Contrairement à l'analyse, qui étudie des phénomènes continus, les mathématiques discrètes s'intéressent aux structures finies ou dénombrables : entiers, graphes, arbres, langages formels, automates et circuits logiques.

Ce cours a été conçu pour les étudiants de première et deuxième année de licence (L1/L2) en mathématiques, en informatique ou dans toute formation scientifique où ces notions interviennent. Aucun prérequis n'est exigé au-delà d'une familiarité raisonnable avec le calcul algébrique et les notions élémentaires d'ensembles.

Objectifs pédagogiques.

- Maîtriser le raisonnement logique et les principales techniques de démonstration.
- Connaître les fondements de la théorie des ensembles, des relations et des fonctions.
- Étudier les structures combinatoires fondamentales : dénombrements, permutations, combinaisons.
- Comprendre les concepts clés de la théorie des graphes.
- S'initier à l'arithmétique modulaire et à ses applications.
- Développer la rigueur mathématique nécessaire à l'informatique théorique.

Organisation du cours. Chaque chapitre suit une progression qui va des définitions et des théorèmes fondamentaux vers des exemples détaillés et des exercices de difficulté croissante, signalée par des étoiles :

★	Exercice d'application directe
★★	Exercice de synthèse
★★★	Exercice d'approfondissement ou de recherche

Les encadrés colorés distinguent visuellement les définitions (bleu), les théorèmes (rouge), les propositions (orange), les lemmes (jaune), les corollaires (vert), les remarques (gris) et les exemples (violet).

Nous espérons que cet ouvrage accompagnera le lecteur dans sa découverte d'un domaine aussi riche que stimulant.

L'auteur

Table des notations

Notation	**Signification**
$\mathbb{N}$	Ensemble des entiers naturels $\{0, 1, 2, \dots\}$
$\mathbb{N}^*$	$\mathbb{N} \setminus \{0\}$
$\mathbb{Z}$	Ensemble des entiers relatifs
$\mathbb{Q}$	Ensemble des nombres rationnels
$\mathbb{R}$	Ensemble des nombres réels
$\mathbb{C}$	Ensemble des nombres complexes
$\mathcal{P}(E)$	Ensemble des parties (ensemble puissance) de E
$\mathrm{card}(E)$, $\lvert E\rvert$	Cardinalité de l'ensemble E
$\emptyset$	Ensemble vide
$\in$, $\notin$	Appartenance, non-appartenance
$\subset$, $\subseteq$	Inclusion stricte, inclusion large
$\cup$, $\cap$	Réunion, intersection
$\setminus$	Différence ensembliste
A^c, $\overline{A}$	Complémentaire de A
$A \times B$	Produit cartésien
$\neg p$, $\neg p$	Négation de p
$p \wedge q$	Conjonction (« et »)
$p \vee q$	Disjonction (« ou »)
$p \Rightarrow q$, $p \to q$	Implication
$p \Leftrightarrow q$, $p \leftrightarrow q$	Équivalence logique
$\forall$	Quantificateur universel (« pour tout »)
$\exists$	Quantificateur existentiel (« il existe »)
$\exists!$	Quantificateur d'unicité
$n!$	Factorielle de n
$\binom{n}{k}$	Coefficient binomial « n parmi k »
$a \mid b$	a divise b
$a \equiv b \pmod{n}$	Congruence modulo n
$\gcd(a, b)$, $\mathrm{pgcd}(a, b)$	Plus grand commun diviseur
$\mathrm{lcm}(a, b)$, $\mathrm{ppcm}(a, b)$	Plus petit commun multiple

Notation	**Signification**
$\lfloor x \rfloor$	Partie entière inférieure
$\lceil x \rceil$	Partie entière supérieure
$\sum, \prod$	Somme, produit
$f \circ g$	Composition de fonctions
$G = (V, E)$	Graphe de sommets V et d'arêtes E

Table des matières

Chapitre 1

Logique propositionnelle et prédicats

Introduction

La logique mathématique est le langage fondamental dans lequel s'expriment toutes les mathématiques. Elle fournit les règles de raisonnement qui garantissent la validité des démonstrations. En informatique, la logique intervient aussi bien dans la conception de circuits numériques que dans la vérification formelle de programmes.

Ce chapitre présente deux niveaux de logique :

(i) la **logique propositionnelle**, qui manipule des propositions atomiques reliées par des connecteurs ;

(ii) la **logique des prédicats**, qui enrichit le formalisme précédent avec des variables et des quantificateurs.

1.1 Propositions et valeurs de vérité

Définition 1.1 (Proposition)**.** Une **proposition** (ou *énoncé*) est une phrase déclarative qui possède exactement une **valeur de vérité** : soit **vrai** (noté V ou 1), soit **faux** (noté F ou 0).

Exemple 1.2 (Propositions)**.** Les phrases suivantes sont des propositions :

(a) « $2 + 3 = 5$ » est une proposition vraie.

(b) « Tout nombre premier est impair » est une proposition fausse (2 est premier et pair).

(c) « Il existe une infinité de nombres premiers » est une proposition vraie.

En revanche, les phrases « Ferme la porte ! » et « $x + 1 = 3$ » (sans préciser x) ne sont *pas* des propositions.

Notation 1.3 (Variables propositionnelles). On désigne les propositions par des lettres minuscules $p, q, r, s, \ldots$ appelées **variables propositionnelles**.

1.2 Connecteurs logiques

À partir de propositions simples, on construit des propositions composées à l'aide de **connecteurs logiques**.

Définition 1.4 (Négation)**.** Soit p une proposition. La **négation** de p, notée $\neg p$, est la proposition dont la valeur de vérité est l'opposée de celle de p.

p	$\neg p$
V	F
F	V

Définition 1.5 (Conjonction)**.** Soient p et q deux propositions. La **conjonction** de p et q, notée $p \wedge q$, est vraie si et seulement si p et q sont toutes deux vraies.

p	q	$p \wedge q$
V	V	V
V	F	F
F	V	F
F	F	F

Définition 1.6 (Disjonction)**.** Soient p et q deux propositions. La **disjonction** (ou inclusif) de p et q, notée $p \vee q$, est vraie si et seulement si au moins l'une des deux propositions est vraie.

p	q	$p \vee q$
V	V	V
V	F	V
F	V	V
F	F	F

Définition 1.7 (Implication)**.** Soient p et q deux propositions. L'**implication** $p \to q$ (lue « p implique q » ou « si p alors q ») est fausse uniquement lorsque p est vraie et q est fausse.

p	q	$p \to q$
V	V	V
V	F	F
F	V	V
F	F	V

On appelle p l'**hypothèse** (ou antécédent) et q la **conclusion** (ou conséquent).

Remarque 1.8 (Implication matérielle). En mathématiques, $p \to q$ est automatiquement vraie dès que p est fausse. Cette convention, dite de l'*implication matérielle*, peut sembler contre-intuitive mais est essentielle à la cohérence du système logique. Par exemple, « si $1 = 2$ alors la Lune est un fromage » est une proposition vraie.

Définition 1.9 (Équivalence logique (biconditionnelle))**.** Soient p et q deux propositions. La **biconditionnelle** $p \leftrightarrow q$ est vraie si et seulement si p et q ont la même valeur de vérité.

p	q	$p \leftrightarrow q$
V	V	V
V	F	F
F	V	F
F	F	V

On dit aussi que p et q sont **logiquement équivalentes** et on écrit $p \equiv q$ ou $p \Leftrightarrow q$.

Exemple 1.10 (Priorité des connecteurs)**.** Par convention, l'ordre de priorité décroissante des connecteurs est :

$$\neg \quad > \quad \wedge \quad > \quad \vee \quad > \quad \to \quad > \quad \leftrightarrow .$$

Ainsi, $\neg p \wedge q \to r$ se lit $((\neg p) \wedge q) \to r$.

1.3 Tables de vérité

Une **table de vérité** énumère systématiquement toutes les combinaisons possibles de valeurs de vérité des variables propositionnelles et donne la valeur de vérité de la proposition composée pour chacune d'elles.

Exemple 1.11 (Table de vérité complète)**.** Construisons la table de vérité de $\varphi = (p \to q) \wedge (\neg q \to \neg p)$.

p	q	$\neg p$	$\neg q$	$p \to q$	$\neg q \to \neg p$
V	V	F	F	V	V
V	F	F	V	F	F
F	V	V	F	V	V
F	F	V	V	V	V

On observe que les colonnes de $p \to q$ et de $\neg q \to \neg p$ sont identiques : il s'agit en fait de la *contraposée*, dont nous reparlerons au efch :demonstration.

1.4 Tautologies, contradictions et équivalences

Définition 1.12 (Tautologie et contradiction)**.** (i) Une proposition composée qui est **toujours vraie**, quelle que soit la valeur de vérité de ses variables, est appelée une **tautologie**.

(ii) Une proposition composée qui est **toujours fausse** est appelée une **contradiction**.

(iii) Une proposition qui n'est ni une tautologie ni une contradiction est dite **contingente**.

Exemple 1.13 (Tautologie classique)**.** La proposition $p \vee \neg p$ est une tautologie (principe du tiers exclu). La proposition $p \wedge \neg p$ est une contradiction.

Définition 1.14 (Équivalence logique)**.** Deux propositions φ et ψ sont **logiquement équivalentes**, noté $\varphi \equiv \psi$, si et seulement si $\varphi \leftrightarrow \psi$ est une tautologie, c'est-à-dire si φ et ψ ont la même valeur de vérité pour toute affectation des variables.

Proposition 1.15 (Équivalences fondamentales)**.** *Pour toutes propositions p, q et r :*

(i) ***Double négation*** *:* $\neg(\neg p) \equiv p$.

(ii) ***Commutativité*** *:* $p \wedge q \equiv q \wedge p$ *et* $p \vee q \equiv q \vee p$.

(iii) ***Associativité*** *:* $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$ *et* $(p \vee q) \vee r \equiv p \vee (q \vee r)$.

(iv) ***Distributivité*** *:* $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$ *et* $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$.

(v) ***Idempotence*** *:* $p \wedge p \equiv p$ *et* $p \vee p \equiv p$.

(vi) ***Absorption*** *:* $p \wedge (p \vee q) \equiv p$ *et* $p \vee (p \wedge q) \equiv p$.

(vii) ***Éléments neutres*** *:* $p \wedge V \equiv p$, $p \vee F \equiv p$.

(viii) ***Éléments absorbants*** *:* $p \wedge F \equiv F$, $p \vee V \equiv V$.

(ix) ***Implication*** *:* $p \to q \equiv \neg p \vee q$.

(x) ***Biconditionnelle*** *:* $p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$.

Démonstration. Chaque équivalence se vérifie par construction de la table de vérité correspondante. À titre d'illustration, démontrons (ix). La table de vérité de $p \to q$ et de $\neg p \vee q$ est :

p	q	$\neg p$	$p \to q$	$\neg p \vee q$
V	V	F	V	V
V	F	F	F	F
F	V	V	V	V
F	F	V	V	V

Les deux dernières colonnes étant identiques, on conclut $p \to q \equiv \neg p \vee q$. □

1.5 Lois de De Morgan

Les lois de De Morgan sont parmi les équivalences les plus utiles en logique et en théorie des ensembles.

Théorème 1.16 (Lois de De Morgan)**.** *Pour toutes propositions p et q :*

(i) $\neg(p \wedge q) \equiv \neg p \vee \neg q$,

(ii) $\neg(p \vee q) \equiv \neg p \wedge \neg q$.

Démonstration. Démontrons (i) par table de vérité.

p	q	$p \wedge q$	$\neg(p \wedge q)$	$\neg p$	$\neg q$	$\neg p \vee \neg q$
V	V	V	F	F	F	F
V	F	F	V	F	V	V
F	V	F	V	V	F	V
F	F	F	V	V	V	V

Les colonnes $\neg(p \wedge q)$ et $\neg p \vee \neg q$ sont identiques, ce qui établit (i).

Démontrons (ii) par table de vérité.

p	q	$p \vee q$	$\neg(p \vee q)$	$\neg p$	$\neg q$	$\neg p \wedge \neg q$
V	V	V	F	F	F	F
V	F	V	F	F	V	F
F	V	V	F	V	F	F
F	F	F	V	V	V	V

Les colonnes $\neg(p \vee q)$ et $\neg p \wedge \neg q$ coïncident, ce qui établit (ii). □

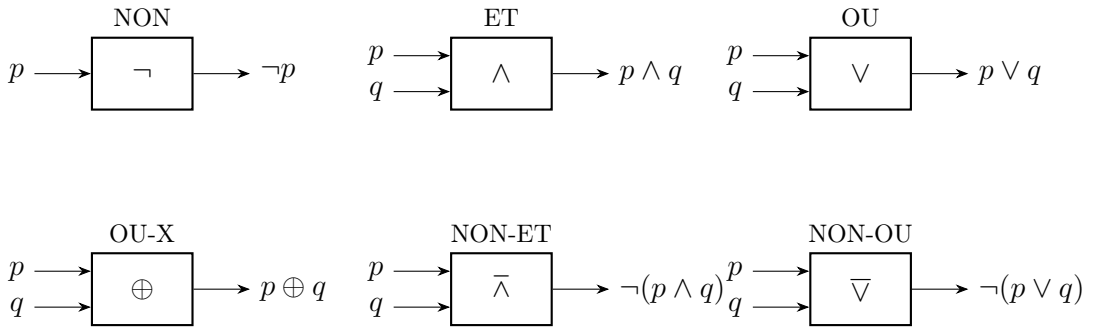
Remarque 1.17 (Extension aux connecteurs généralisés). Les lois de De Morgan se généralisent à un nombre fini quelconque de propositions :

$$\neg\big(p_1 \wedge p_2 \wedge \cdots \wedge p_n\big) \equiv \neg p_1 \vee \neg p_2 \vee \cdots \vee \neg p_n,$$

$$\neg\big(p_1 \vee p_2 \vee \cdots \vee p_n\big) \equiv \neg p_1 \wedge \neg p_2 \wedge \cdots \wedge \neg p_n.$$

1.6 Portes logiques — une perspective informatique

Les connecteurs logiques sont matérialisés dans les circuits électroniques sous forme de **portes logiques**. Voici les principales portes avec leurs symboles standard :



Remarque 1.18 (Universalité de NAND). La porte NAND est dite *universelle* : tout circuit logique peut être réalisé en utilisant uniquement des portes NAND. De même pour la porte NOR.

1.7 Logique des prédicats

La logique propositionnelle ne permet pas d'exprimer des énoncés portant sur des variables, comme « pour tout entier n, $n^2 \geq 0$ ». La **logique des prédicats** enrichit le formalisme en introduisant des variables et des quantificateurs.

Définition 1.19 (Prédicat)**.** Un **prédicat** (ou *fonction propositionnelle*) est une expression $P(x_1, x_2, \ldots, x_n)$ contenant des variables libres, qui devient une proposition dès que l'on affecte des valeurs aux variables, à condition de préciser un **domaine de discours** (ou **univers**).

Exemple 1.20 (Prédicats)**.** (a) $P(x)$: « x est un nombre premier » est un prédicat sur $\mathbb{N}$. Alors $P(7)$ est vrai et $P(10)$ est faux.

(b) $Q(x, y)$: « $x + y = 10$ » est un prédicat à deux variables sur $\mathbb{Z}$. Alors $Q(3, 7)$ est vrai et $Q(2, 5)$ est faux.

1.7.1 Quantificateurs

Définition 1.21 (Quantificateur universel)**.** Soit $P(x)$ un prédicat de domaine D. L'énoncé

$$\forall x \in D,\ P(x)$$

(lu « pour tout x dans D, $P(x)$ ») est vrai si et seulement si $P(a)$ est vrai pour **chaque** élément $a \in D$.

Définition 1.22 (Quantificateur existentiel)**.** Soit $P(x)$ un prédicat de domaine D. L'énoncé

$$\exists x \in D,\ P(x)$$

(lu « il existe x dans D tel que $P(x)$ ») est vrai si et seulement si $P(a)$ est vrai pour **au moins un** élément $a \in D$.

Exemple 1.23 (Quantificateurs sur $\mathbb{N}$). (a) $\forall n \in \mathbb{N},\ n + 0 = n$ est vrai.
(b) $\exists n \in \mathbb{N},\ n^2 = 2$ est faux (car $\sqrt{2} \notin \mathbb{N}$).
(c) $\exists n \in \mathbb{N},\ n^2 = 4$ est vrai ($n = 2$).

Définition 1.24 (Quantificateur d'unicité). L'énoncé $\exists!\, x \in D,\ P(x)$ (lu « il existe un unique x dans D tel que $P(x)$ ») signifie qu'il existe exactement un élément de D satisfaisant P. Formellement :

$$\exists x \in D,\ P(x)\ \wedge\ \big(\forall y \in D,\ P(y) \to y = x\big).$$

1.7.2 Négation des énoncés quantifiés

Théorème 1.25 (Négation des quantificateurs). *Soit $P(x)$ un prédicat de domaine D. Alors :*
(i) $\neg\big(\forall x \in D,\ P(x)\big)\ \equiv\ \exists x \in D,\ \neg P(x).$
(ii) $\neg\big(\exists x \in D,\ P(x)\big)\ \equiv\ \forall x \in D,\ \neg P(x).$

Démonstration. (i) L'énoncé $\forall x \in D,\ P(x)$ est faux si et seulement s'il existe au moins un élément $a \in D$ pour lequel $P(a)$ est faux, c'est-à-dire $\neg P(a)$ est vrai. Cela revient exactement à dire $\exists x \in D,\ \neg P(x)$.

(ii) L'énoncé $\exists x \in D,\ P(x)$ est faux si et seulement si aucun élément de D ne satisfait P, c'est-à-dire si $\neg P(a)$ est vrai pour tout $a \in D$. Cela donne $\forall x \in D,\ \neg P(x)$. □

Exemple 1.26 (Négation d'un énoncé). Négations la proposition « tout nombre réel positif admet une racine carrée » :

$$\neg\big(\forall x \in \mathbb{R},\ x \geq 0 \to \exists y \in \mathbb{R},\ y^2 = x\big)\ \equiv\ \exists x \in \mathbb{R},\ x \geq 0\ \wedge\ \forall y \in \mathbb{R},\ y^2 \neq x.$$

La négation dit qu'il existe un réel positif qui n'a pas de racine carrée réelle. (Cet énoncé est faux, car la proposition initiale est vraie.)

1.7.3 Quantificateurs emboîtés

Lorsque plusieurs quantificateurs interviennent, l'**ordre** dans lequel ils apparaissent est crucial.

Proposition 1.27 (Commutation de quantificateurs de même type). *Pour tout prédicat $P(x, y)$:*
(i) $\forall x,\ \forall y,\ P(x, y)\ \equiv\ \forall y,\ \forall x,\ P(x, y).$
(ii) $\exists x,\ \exists y,\ P(x, y)\ \equiv\ \exists y,\ \exists x,\ P(x, y).$
En revanche, en général :

$$\forall x,\ \exists y,\ P(x, y)\ \not\equiv\ \exists y,\ \forall x,\ P(x, y).$$

Exemple 1.28 (Importance de l'ordre)**.** Sur $\mathbb{R}$:

(a) $\forall x \in \mathbb{R},\ \exists y \in \mathbb{R},\ x + y = 0$ est **vrai** (prendre $y = -x$).

(b) $\exists y \in \mathbb{R},\ \forall x \in \mathbb{R},\ x + y = 0$ est **faux** (aucun y fixé ne convient pour tout x).

Remarque 1.29 (Négation de quantificateurs emboîtés)*.* Pour nier un énoncé à quantificateurs multiples, on inverse chaque quantificateur de gauche à droite et on nie le prédicat final. Par exemple :

$$\neg\big(\forall x,\ \exists y,\ P(x,y)\big) \ \equiv\ \exists x,\ \forall y,\ \neg P(x,y).$$

1.8 Exercices

Exercice 1.1 (★)**.** Construire la table de vérité de $(p \to q) \to (\neg q \to \neg p)$. Que constatez-vous ?

Exercice 1.2 (★)**.** Montrer par table de vérité que $p \to (q \to r) \equiv (p \wedge q) \to r$.

Exercice 1.3 (★)**.** Écrire la négation de chacune des propositions suivantes :

(a) $\forall n \in \mathbb{N},\ n^2 \geq n$.

(b) $\exists x \in \mathbb{R},\ x^2 + x + 1 = 0$.

(c) $\forall \varepsilon > 0,\ \exists N \in \mathbb{N},\ \forall n \geq N,\ |u_n - \ell| < \varepsilon$.

Exercice 1.4 (★★)**.** Étendre les lois de De Morgan à trois propositions. Démontrer que :

$$\neg(p \wedge q \wedge r) \equiv \neg p \vee \neg q \vee \neg r.$$

Exercice 1.5 (★★)**.** Simplifier la proposition suivante en utilisant les équivalences logiques de la efprop :equiv-fondamentales :

$$\big[(p \vee q) \wedge (p \vee \neg q)\big] \vee q.$$

Exercice 1.6 (★★)**.** On définit $P(x, y)$ comme « $x \leq y$ » sur $\mathbb{N}$. Déterminer la valeur de vérité de :

(a) $\forall x \in \mathbb{N},\ \exists y \in \mathbb{N},\ P(x,y)$.

(b) $\exists y \in \mathbb{N},\ \forall x \in \mathbb{N},\ P(x,y)$.

(c) $\forall x \in \mathbb{N},\ \forall y \in \mathbb{N},\ P(x,y) \vee P(y,x)$.

Exercice 1.7 (★★★)**.** Un ensemble de connecteurs est dit **fonctionnellement complet** si toute fonction booléenne peut s'exprimer uniquement à l'aide de ces connecteurs. Montrer que $\{\neg, \wedge\}$ est fonctionnellement complet. *Indication : exprimer $p \vee q$ en fonction de $\neg$ et $\wedge$.*

Exercice 1.8 (★★★)**.** Montrer que toute fonction booléenne peut être réalisée uniquement avec la porte NAND (notée $|$, définie par $p \mid q \equiv \neg(p \wedge q)$). *Indication : exprimer $\neg p$ et $p \wedge q$ à l'aide de $|$.*

Résumé du chapitre

— Une **proposition** est un énoncé vrai ou faux. On combine les propositions avec les connecteurs $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$.

— Les **tables de vérité** permettent de déterminer la valeur de vérité de toute proposition composée.

— Une **tautologie** est toujours vraie ; une **contradiction** est toujours fausse.

— Les **lois de De Morgan** relient négation, conjonction et disjonction : $\neg(p \wedge q) \equiv \neg p \vee \neg q$ et $\neg(p \vee q) \equiv \neg p \wedge \neg q$.

— Un **prédicat** est un énoncé contenant des variables libres. Les **quantificateurs** $\forall$ et $\exists$ transforment un prédicat en proposition.

— Pour nier un énoncé quantifié, on échange $\forall$ et $\exists$ puis on nie le prédicat.

— L'ordre des quantificateurs de types différents est crucial : $\forall x\, \exists y$ ne signifie pas la même chose que $\exists y\, \forall x$.

Chapitre 2

Techniques de démonstration

Introduction

Savoir énoncer un théorème ne suffit pas : il faut aussi être capable de le *démontrer*. La démonstration est le processus par lequel on établit la vérité d'un énoncé mathématique à partir d'axiomes, de définitions et de théorèmes déjà établis, en utilisant des règles de déduction logiquement valides.

Ce chapitre présente les techniques de démonstration les plus courantes et les plus puissantes. La maîtrise de ces techniques est indispensable non seulement en mathématiques mais aussi en informatique, où elles servent à prouver la correction d'algorithmes, la terminaison de programmes et la validité de protocoles.

2.1 Démonstration directe

Définition 2.1 (Démonstration directe)**.** Une **démonstration directe** d'un énoncé $p \to q$ consiste à supposer que p est vrai, puis à en déduire que q est vrai par une chaîne d'implications logiques.

Théorème 2.2 (Somme de deux nombres pairs)**.** *La somme de deux nombres entiers pairs est paire.*

Démonstration. Soient a et b deux entiers pairs. Par définition, il existe $k, \ell \in \mathbb{Z}$ tels que $a = 2k$ et $b = 2\ell$. Alors :

$$a + b = 2k + 2\ell = 2(k + \ell).$$

Comme $k + \ell \in \mathbb{Z}$, on conclut que $a + b$ est pair. □

Théorème 2.3 (Produit d'un pair et d'un entier)**.** *Si a est un entier pair, alors pour tout entier b, le produit ab est pair.*

Démonstration. Soit a un entier pair : il existe $k \in \mathbb{Z}$ tel que $a = 2k$. Pour tout $b \in \mathbb{Z}$:

$$ab = (2k)b = 2(kb).$$

Comme $kb \in \mathbb{Z}$, le produit ab est pair. □

Théorème 2.4 (Carré d'un impair)**.** *Le carré de tout nombre impair est impair.*

Démonstration. Soit n un entier impair. Il existe $k \in \mathbb{Z}$ tel que $n = 2k + 1$. Alors :

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

Comme $2k^2 + 2k \in \mathbb{Z}$, l'entier n^2 est de la forme $2m + 1$ avec $m = 2k^2 + 2k$, donc n^2 est impair. □

Exemple 2.5 (Divisibilité)**.** Montrons directement que pour tout entier n, si $6 \mid n$ alors $3 \mid n$.

Démonstration. Supposons $6 \mid n$. Il existe $k \in \mathbb{Z}$ tel que $n = 6k = 3(2k)$. Comme $2k \in \mathbb{Z}$, on a bien $3 \mid n$. □

2.2 Démonstration par l'absurde

Définition 2.6 (Démonstration par l'absurde)**.** Pour démontrer un énoncé φ, une **démonstration par l'absurde** consiste à supposer $\neg\varphi$, puis à en déduire une contradiction (une proposition de la forme $\psi \wedge \neg\psi$). On conclut alors que φ est vrai.

Ce raisonnement repose sur l'équivalence : $\varphi \equiv \neg(\neg\varphi)$ et sur le fait qu'un énoncé dont la négation mène à une contradiction doit être vrai.

Théorème 2.7 (Irrationalité de $\sqrt{2}$)**.** *Le nombre $\sqrt{2}$ est irrationnel.*

Démonstration. Supposons, par l'absurde, que $\sqrt{2}$ est rationnel. Alors il existe $p, q \in \mathbb{Z}$ avec $q \neq 0$ et $\gcd(p, q) = 1$ (fraction irréductible) tels que $\sqrt{2} = \dfrac{p}{q}$.

En élevant au carré : $2 = \dfrac{p^2}{q^2}$, donc $p^2 = 2q^2$.

Ainsi p^2 est pair, ce qui implique que p est pair (car si p était impair, p^2 serait impair d'après le efthm :carre-impair). On écrit $p = 2k$ pour un certain $k \in \mathbb{Z}$.

Substituant : $(2k)^2 = 2q^2$, soit $4k^2 = 2q^2$, d'où $q^2 = 2k^2$. Donc q^2 est pair, et par le même argument, q est pair.

Mais alors p et q sont tous deux pairs, ce qui contredit l'hypothèse $\gcd(p, q) = 1$. Cette contradiction montre que $\sqrt{2}$ est irrationnel. □

Théorème 2.8 (Infinité des nombres premiers)**.** *Il existe une infinité de nombres premiers.*

Démonstration. Supposons, par l'absurde, qu'il n'existe qu'un nombre fini de nombres premiers : $p_1, p_2, \ldots, p_n$. Considérons l'entier :

$$N = p_1 \cdot p_2 \cdots p_n + 1.$$

Puisque $N > 1$, par le théorème fondamental de l'arithmétique, N admet au moins un diviseur premier p. Or, pour tout $i \in \{1, \ldots, n\}$, on a $N \equiv 1 \pmod{p_i}$, donc $p_i \nmid N$. Ainsi

p n'est aucun des p_i, ce qui contredit l'hypothèse que $p_1, \ldots, p_n$ sont *tous* les nombres premiers. □

Exemple 2.9 (Absence de plus petit rationnel strictement positif)**.** Montrons par l'absurde qu'il n'existe pas de plus petit nombre rationnel strictement positif.

Démonstration. Supposons qu'un tel nombre $r \in \mathbb{Q}$ existe, avec $r > 0$ et $r \leq s$ pour tout $s \in \mathbb{Q}$ avec $s > 0$. Considérons $r' = \dfrac{r}{2}$. Alors $r' \in \mathbb{Q}$, $r' > 0$ et $r' < r$, ce qui contredit la minimalité de r. □

2.3 Démonstration par contraposée

Définition 2.10 (Contraposée)**.** La **contraposée** de l'implication $p \to q$ est l'implication $\neg q \to \neg p$. On a l'équivalence logique :

$$(p \to q) \equiv (\neg q \to \neg p).$$

Une **démonstration par contraposée** de $p \to q$ consiste donc à supposer $\neg q$ et à en déduire $\neg p$.

Remarque 2.11 (Contraposée vs. absurde). La preuve par contraposée est un cas particulier de la preuve par l'absurde (on suppose p et $\neg q$, et on obtient une contradiction avec p). Cependant, la contraposée a l'avantage d'être plus directe : on part de $\neg q$ et on arrive à $\neg p$ sans chercher explicitement une contradiction.

Théorème 2.12 (Critère de parité du carré)**.** *Pour tout entier n, si n^2 est pair alors n est pair.*

Démonstration. Nous démontrons la contraposée : si n est impair, alors n^2 est impair. C'est exactement le efthm :carre-impair, qui a déjà été établi par preuve directe. □

Théorème 2.13 (Condition de divisibilité)**.** *Pour tous entiers a et b, si ab est impair alors a est impair et b est impair.*

Démonstration. Par contraposée, supposons que a est pair ou b est pair (c'est-à-dire $\neg(a \text{ impair} \wedge b \text{ impair})$). Supposons, sans perte de généralité, que a est pair : $a = 2k$ pour un certain $k \in \mathbb{Z}$. Alors $ab = 2kb = 2(kb)$, donc ab est pair. On a bien montré que $\neg(a \text{ impair} \wedge b \text{ impair}) \to ab$ pair. □

Exemple 2.14 (Irrationnalité par contraposée)**.** Montrons que pour tout entier positif n, si $\sqrt{n}$ est rationnel alors $\sqrt{n}$ est un entier.

Démonstration par contraposée. On montre : si $\sqrt{n}$ n'est pas un entier, alors $\sqrt{n}$ est irrationnel. Supposons $\sqrt{n} \notin \mathbb{Z}$ et supposons par l'absurde que $\sqrt{n} = \frac{p}{q}$ avec $q > 1$ et $\gcd(p, q) = 1$. Alors $n = \frac{p^2}{q^2}$, donc $nq^2 = p^2$. Soit r un facteur premier de q ; alors

$r \mid q^2$ donc $r \mid p^2$, ce qui implique $r \mid p$ (par le lemme d'Euclide). Mais cela contredit $\gcd(p, q) = 1$. □

2.4 Récurrence mathématique

La récurrence est l'une des méthodes de démonstration les plus importantes en mathématiques discrètes. Elle exploite la structure bien ordonnée de $\mathbb{N}$.

2.4.1 Récurrence simple (faible)

Théorème 2.15 (Principe de récurrence simple)**.** *Soit $P(n)$ une propriété définie pour tout $n \geq n_0$ ($n_0 \in \mathbb{N}$). Si :*

(i) ***Base*** *: $P(n_0)$ est vraie, et*

(ii) ***Hérédité*** *: pour tout $n \geq n_0$, $P(n) \to P(n+1)$,*

alors $P(n)$ est vraie pour tout $n \geq n_0$.

Remarque 2.16 (Analogie du domino). La récurrence s'apparente à une file infinie de dominos : si le premier domino tombe (*base*), et si chaque domino en tombant fait tomber le suivant (*hérédité*), alors tous les dominos tombent.

Théorème 2.17 (Somme des n premiers entiers)**.** *Pour tout $n \in \mathbb{N}^*$:*

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}.$$

Démonstration. Démonstration par récurrence sur n.

Base ($n = 1$) : $\displaystyle\sum_{k=1}^{1} k = 1 = \frac{1 \cdot 2}{2}$. ✓

Hérédité. Supposons que la formule est vraie pour un certain $n \geq 1$ (**hypothèse de récurrence**). Montrons qu'elle est vraie pour $n + 1$:

$$\begin{aligned}
\sum_{k=1}^{n+1} k &= \left(\sum_{k=1}^{n} k\right) + (n+1) \\
&= \frac{n(n+1)}{2} + (n+1) \quad \text{(par hypothèse de récurrence)} \\
&= \frac{n(n+1) + 2(n+1)}{2} \\
&= \frac{(n+1)(n+2)}{2}.
\end{aligned}$$

C'est bien la formule au rang $n + 1$. Par le principe de récurrence, la propriété est vraie pour tout $n \geq 1$. □

Théorème 2.18 (Somme géométrique)**.** *Pour tout $r \neq 1$ et tout $n \in \mathbb{N}$:*

$$\sum_{k=0}^{n} r^k = \frac{1 - r^{n+1}}{1 - r}.$$

Démonstration. Par récurrence sur n.

Base $(n = 0)$: $\sum_{k=0}^{0} r^k = 1 = \frac{1 - r}{1 - r}$. ✓

Hérédité. Supposons la formule vraie au rang n. Alors :

$$\begin{aligned}\sum_{k=0}^{n+1} r^k &= \left(\sum_{k=0}^{n} r^k\right) + r^{n+1} = \frac{1 - r^{n+1}}{1 - r} + r^{n+1} \\ &= \frac{1 - r^{n+1} + r^{n+1}(1 - r)}{1 - r} = \frac{1 - r^{n+1} + r^{n+1} - r^{n+2}}{1 - r} \\ &= \frac{1 - r^{n+2}}{1 - r}.\end{aligned}$$

C'est la formule au rang $n + 1$, ce qui achève la récurrence. □

Théorème 2.19 (Inégalité de Bernoulli)**.** *Pour tout $x \geq -1$ et tout $n \in \mathbb{N}$:*

$$(1 + x)^n \geq 1 + nx.$$

Démonstration. Par récurrence sur n.

Base $(n = 0)$: $(1 + x)^0 = 1 \geq 1 + 0 = 1$. ✓

Hérédité. Supposons $(1 + x)^n \geq 1 + nx$ pour un certain $n \geq 0$. Puisque $x \geq -1$, on a $1 + x \geq 0$, donc :

$$\begin{aligned}(1 + x)^{n+1} &= (1 + x)^n \cdot (1 + x) \\ &\geq (1 + nx)(1 + x) \quad \text{(par hypothèse de récurrence et } 1 + x \geq 0) \\ &= 1 + nx + x + nx^2 \\ &= 1 + (n + 1)x + nx^2 \\ &\geq 1 + (n + 1)x \quad (\text{car } nx^2 \geq 0).\end{aligned}$$

La propriété est donc héréditaire. □

2.4.2 Récurrence forte

Théorème 2.20 (Principe de récurrence forte)**.** *Soit $P(n)$ une propriété définie pour tout $n \geq n_0$. Si :*

(i) ***Base*** *: $P(n_0)$ est vraie (éventuellement plusieurs cas de base), et*

(ii) ***Hérédité forte*** *: pour tout $n \geq n_0$, si $P(k)$ est vraie pour tout k avec $n_0 \leq k \leq n$, alors $P(n + 1)$ est vraie,*

alors $P(n)$ est vraie pour tout $n \geq n_0$.

Remarque 2.21 (Récurrence simple vs. forte). En récurrence simple, l'hypothèse au rang n porte uniquement sur $P(n)$. En récurrence forte, elle porte sur $P(n_0), P(n_0+1), \ldots, P(n)$ simultanément. La récurrence forte est particulièrement utile lorsque $P(n+1)$ dépend de plusieurs valeurs antérieures, et pas seulement de $P(n)$.

Théorème 2.22 (Théorème fondamental de l'arithmétique — existence)**.** *Tout entier $n \geq 2$ peut s'écrire comme produit de nombres premiers.*

Démonstration. Par récurrence forte sur $n \geq 2$.

Base ($n = 2$) : 2 est premier, donc 2 est un produit de nombres premiers (un seul facteur). ✓

Hérédité forte. Soit $n \geq 2$ et supposons que tout entier k avec $2 \leq k \leq n$ s'écrit comme produit de nombres premiers. Considérons $n+1$.

— Si $n+1$ est premier, c'est un produit de nombres premiers. ✓

— Si $n+1$ n'est pas premier, alors $n+1 = ab$ avec $2 \leq a, b \leq n$. Par hypothèse de récurrence forte, a et b s'écrivent chacun comme produit de nombres premiers. Donc $n+1 = ab$ est un produit de nombres premiers. ✓

Par le principe de récurrence forte, tout entier $n \geq 2$ est un produit de nombres premiers. □

Exemple 2.23 (Suite de Fibonacci)**.** Soit $(F_n)_{n\geq 0}$ la suite de Fibonacci définie par $F_0 = 0$, $F_1 = 1$ et $F_n = F_{n-1} + F_{n-2}$ pour $n \geq 2$. Montrons par récurrence forte que $F_n < 2^n$ pour tout $n \geq 0$.

Démonstration. **Bases** : $F_0 = 0 < 1 = 2^0$ et $F_1 = 1 < 2 = 2^1$. ✓

Hérédité forte. Soit $n \geq 1$ et supposons $F_k < 2^k$ pour tout $0 \leq k \leq n$. Alors :

$$F_{n+1} = F_n + F_{n-1} < 2^n + 2^{n-1} = 2^{n-1}(2+1) = 3 \cdot 2^{n-1} < 4 \cdot 2^{n-1} = 2^{n+1}.$$

Donc $F_{n+1} < 2^{n+1}$. □

2.4.3 Récurrence structurelle (mention)

Remarque 2.24 (Récurrence structurelle). La récurrence mathématique s'applique aux entiers naturels. En informatique, on utilise souvent la **récurrence structurelle**, qui généralise le principe à des structures définies inductivement (listes, arbres, expressions, etc.). Le principe est le même :

(i) on montre la propriété pour les cas de base de la structure ;

(ii) on montre que si la propriété est vraie pour les sous-structures, elle l'est aussi pour la structure construite à partir d'elles.

Par exemple, pour prouver une propriété sur les arbres binaires, on la démontre pour l'arbre vide (base), puis on montre que si elle est vraie pour les sous-arbres gauche et droit, elle l'est pour l'arbre tout entier (hérédité).

2.5 Principe des tiroirs de Dirichlet

Théorème 2.25 (Principe des tiroirs — forme simple)**.** *Si $n+1$ objets (ou plus) sont répartis dans n tiroirs, alors au moins un tiroir contient au moins deux objets.*

Démonstration. Par l'absurde. Supposons que chacun des n tiroirs contient au plus un objet. Alors le nombre total d'objets est au plus $n \cdot 1 = n$, ce qui contredit l'hypothèse de disposer de $n+1$ objets (ou plus). Donc au moins un tiroir contient au moins deux objets. □

Théorème 2.26 (Principe des tiroirs — forme généralisée)**.** *Si N objets sont répartis dans k tiroirs, alors au moins un tiroir contient au moins $\left\lceil \frac{N}{k} \right\rceil$ objets.*

Démonstration. Par l'absurde. Supposons que chaque tiroir contient au plus $\lceil \frac{N}{k} \rceil - 1$ objets. Le nombre total d'objets serait au plus :

$$k \cdot \left(\left\lceil \frac{N}{k} \right\rceil - 1 \right) < k \cdot \left(\frac{N}{k} + 1 - 1 \right) = N,$$

où l'on a utilisé $\lceil x \rceil < x + 1$. Cela contredit l'hypothèse de disposer de N objets. □

Exemple 2.27 (Anniversaires)**.** Dans un groupe de 367 personnes, au moins deux personnes partagent le même jour d'anniversaire. En effet, il y a au plus 366 jours possibles dans une année (en comptant le 29 février), et $367 > 366$. Par le principe des tiroirs, au moins un « tiroir » (jour de l'année) contient au moins deux personnes.

Exemple 2.28 (Chaussettes)**.** Un tiroir contient 10 chaussettes rouges et 10 chaussettes bleues mélangées. Combien faut-il en tirer (dans l'obscurité) pour être sûr d'avoir au moins deux chaussettes de la même couleur ?

Les « tiroirs » sont les 2 couleurs. Par le principe des tiroirs, il suffit de tirer $2 + 1 = 3$ chaussettes.

Théorème 2.29 (Application classique — sous-ensemble de somme divisible)**.** *Soit $n \geq 1$. Parmi n entiers quelconques $a_1, a_2, \ldots, a_n$, il existe un sous-ensemble contigu $\{a_{i+1}, a_{i+2}, \ldots, a_j\}$ dont la somme est divisible par n.*

Démonstration. Considérons les n sommes partielles :

$$S_k = a_1 + a_2 + \cdots + a_k, \quad k = 1, 2, \ldots, n.$$

Examinons les restes de $S_1, S_2, \ldots, S_n$ modulo n. Il y a n restes possibles : $0, 1, \ldots, n-1$.

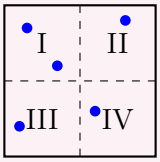
- Si l'un des S_k satisfait $S_k \equiv 0 \pmod{n}$, alors $a_1 + \cdots + a_k$ est divisible par n et on a terminé.
- Sinon, les n restes $S_1 \bmod n, \ldots, S_n \bmod n$ prennent des valeurs dans $\{1, 2, \ldots, n-1\}$ (seulement $n-1$ valeurs possibles). Par le principe des tiroirs, il existe $i < j$ tels que

$S_i \equiv S_j \pmod{n}$. Alors :

$$S_j - S_i = a_{i+1} + a_{i+2} + \cdots + a_j \equiv 0 \pmod{n}. \qquad \square$$

Exemple 2.30 (Points dans un carré)**.** On place 5 points dans un carré de côté 1. Montrons que deux d'entre eux sont à distance au plus $\frac{\sqrt{2}}{2}$.

Démonstration. Découpons le carré en 4 petits carrés de côté $\frac{1}{2}$.



Nous avons 5 points et 4 sous-carrés. Par le principe des tiroirs, au moins un sous-carré contient au moins 2 points. La diagonale d'un carré de côté $\frac{1}{2}$ est $\frac{\sqrt{2}}{2}$, ce qui est la distance maximale entre deux points d'un tel sous-carré. Donc deux points du même sous-carré sont à distance au plus $\frac{\sqrt{2}}{2}$. $\square$

2.6 Principe du bon ordre

Théorème 2.31 (Principe du bon ordre de $\mathbb{N}$)**.** *Toute partie non vide de $\mathbb{N}$ possède un plus petit élément.*

Remarque 2.32 (Lien avec la récurrence). Le principe du bon ordre et le principe de récurrence sont logiquement équivalents : on peut démontrer chacun à partir de l'autre. Le principe du bon ordre fournit une méthode de démonstration alternative : pour montrer qu'une propriété $P(n)$ est vraie pour tout $n \in \mathbb{N}$, on peut supposer que l'ensemble $S = \{n \in \mathbb{N} : \neg P(n)\}$ est non vide et considérer son plus petit élément, pour obtenir une contradiction.

Théorème 2.33 (Division euclidienne)**.** *Pour tous entiers $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$, il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que :*

$$a = bq + r \quad \textit{avec} \quad 0 \leq r < b.$$

Démonstration. **Existence.** Considérons l'ensemble :

$$S = \{a - bk : k \in \mathbb{Z}\} \cap \mathbb{N} = \{a - bk : k \in \mathbb{Z},\ a - bk \geq 0\}.$$

S est non vide : si $a \geq 0$, on prend $k = 0$ et $a - b \cdot 0 = a \geq 0$; si $a < 0$, on prend $k = a$ (par exemple) et $a - ba = a(1 - b) \geq 0$ car $a < 0$ et $1 - b \leq 0$. Par le principe du bon ordre, S possède un plus petit élément $r = a - bq$ pour un certain $q \in \mathbb{Z}$.

On a $r \geq 0$ par construction. Montrons $r < b$. Si $r \geq b$, alors $r - b = a - b(q + 1) \geq 0$, donc $r - b \in S$ et $r - b < r$, ce qui contredit la minimalité de r. Donc $0 \leq r < b$.

Unicité. Supposons $a = bq_1 + r_1 = bq_2 + r_2$ avec $0 \leq r_1, r_2 < b$. Alors $b(q_1 - q_2) = r_2 - r_1$. Ainsi $b \mid (r_2 - r_1)$. Or $|r_2 - r_1| < b$ (car $0 \leq r_1, r_2 < b$), donc $r_2 - r_1 = 0$, d'où $r_1 = r_2$ et $q_1 = q_2$. □

Exemple 2.34 (Application du bon ordre)**.** Montrons que $\sqrt{3}$ est irrationnel en utilisant le principe du bon ordre.

Démonstration. Supposons $\sqrt{3} \in \mathbb{Q}$. Alors l'ensemble :

$$S = \left\{ n \in \mathbb{N}^* : n\sqrt{3} \in \mathbb{N}^* \right\}$$

est non vide (il contient le dénominateur d'une écriture fractionnaire de $\sqrt{3}$). Par le principe du bon ordre, S possède un plus petit élément m. Posons $m' = m\sqrt{3} - m = m(\sqrt{3} - 1)$. Puisque $1 < \sqrt{3} < 2$, on a $0 < \sqrt{3} - 1 < 1$, donc $0 < m' < m$. De plus :

$$m'\sqrt{3} = m(\sqrt{3} - 1)\sqrt{3} = m(3 - \sqrt{3}) = 3m - m\sqrt{3}.$$

Or $m\sqrt{3} \in \mathbb{N}^*$ (puisque $m \in S$), donc $m'\sqrt{3} = 3m - m\sqrt{3} \in \mathbb{Z}$. Comme $m' > 0$ et $\sqrt{3} > 0$, on a $m'\sqrt{3} > 0$, donc $m'\sqrt{3} \in \mathbb{N}^*$. Ainsi $m' \in S$ avec $m' < m$, ce qui contredit la minimalité de m. □

2.7 Exercices

Démonstration directe

Exercice 2.1 (★)**.** Démontrer directement que pour tout entier n, si n est pair, alors n^2 est pair.

Exercice 2.2 (★)**.** Montrer que la somme de trois entiers consécutifs est toujours divisible par 3.

Exercice 2.3 (★★)**.** Montrer que pour tous réels $a, b \geq 0$, on a $\dfrac{a+b}{2} \geq \sqrt{ab}$ (inégalité arithmético-géométrique).

Démonstration par l'absurde

Exercice 2.4 (★)**.** Montrer par l'absurde que $\sqrt{3}$ est irrationnel.

Exercice 2.5 (★★)**.** Montrer qu'il n'existe pas d'entiers a et b tels que $a^2 = 4b + 2$.

Exercice 2.6 (★★)**.** Montrer par l'absurde que si a et b sont des réels tels que $a + b$ est irrationnel, alors a est irrationnel ou b est irrationnel.

Démonstration par contraposée

Exercice 2.7 (★)**.** Montrer par contraposée : pour tout entier n, si n^2 est impair alors n est impair.

Exercice 2.8 (★★)**.** Montrer par contraposée : pour tous réels x et y, si xy est irrationnel, alors x est irrationnel ou y est irrationnel.

Récurrence

Exercice 2.9 (★)**.** Montrer par récurrence que pour tout $n \geq 1$:

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}.$$

Exercice 2.10 (★)**.** Montrer par récurrence que pour tout $n \geq 1$:

$$\sum_{k=1}^{n} (2k-1) = n^2.$$

Exercice 2.11 (★★)**.** Montrer par récurrence que $n! \geq 2^{n-1}$ pour tout $n \geq 1$.

Exercice 2.12 (★★)**.** Montrer par récurrence forte que tout entier $n \geq 2$ est divisible par un nombre premier.

Exercice 2.13 (★★★)**.** Soit (F_n) la suite de Fibonacci. Montrer par récurrence forte que :

$$F_n = \frac{\varphi^n - \psi^n}{\sqrt{5}}, \quad \text{où} \quad \varphi = \frac{1+\sqrt{5}}{2}, \quad \psi = \frac{1-\sqrt{5}}{2}.$$

Indication : vérifier que $\varphi^2 = \varphi + 1$ *et* $\psi^2 = \psi + 1$.

Principe des tiroirs

Exercice 2.14 (★)**.** Montrer que dans un groupe de 13 personnes, au moins deux sont nées le même mois.

Exercice 2.15 (★★)**.** Soit A un sous-ensemble de $\{1, 2, \ldots, 2n\}$ contenant $n+1$ éléments. Montrer que A contient deux éléments dont l'un divise l'autre.

Exercice 2.16 (★★★)**.** On choisit $n+1$ entiers dans l'ensemble $\{1, 2, \ldots, 2n\}$. Montrer qu'il en existe deux dont la différence vaut exactement 1. *Indication : considérer les « tiroirs »* $\{1,2\}, \{3,4\}, \ldots, \{2n-1, 2n\}$.

Exercice 2.17 (★★★)**.** Soit $(a_1, a_2, \ldots, a_{n^2+1})$ une suite de n^2+1 réels distincts. Montrer qu'elle contient soit une sous-suite croissante de longueur $n+1$, soit une sous-suite décroissante de longueur $n+1$. *Indication : associer à chaque* a_i *la longueur de la plus longue sous-suite croissante commençant en* a_i.

Résumé du chapitre

- La **démonstration directe** de $p \to q$ suppose p vrai et en déduit q par une chaîne logique.
- La **démonstration par l'absurde** suppose $\neg\varphi$ et aboutit à une contradiction, prouvant ainsi φ.
- La **démonstration par contraposée** de $p \to q$ consiste à démontrer $\neg q \to \neg p$.
- La **récurrence simple** : on montre $P(n_0)$ (base) et $P(n) \Rightarrow P(n+1)$ (hérédité).
- La **récurrence forte** : l'hypothèse porte sur $P(n_0), \ldots, P(n)$ pour démontrer $P(n+1)$.

— La **récurrence structurelle** généralise la récurrence aux structures définies inductivement.

— Le **principe des tiroirs** (Dirichlet) : $n + 1$ objets dans n tiroirs impliquent un tiroir avec au moins deux objets. Forme généralisée : au moins $\lceil N/k \rceil$ objets dans un tiroir.

— Le **principe du bon ordre** : toute partie non vide de $\mathbb{N}$ a un plus petit élément. Ce principe est équivalent au principe de récurrence.

Chapitre 3

Ensembles, Relations, Fonctions

« La théorie des ensembles est le langage universel des mathématiques. »
— Georg Cantor

Ce chapitre présente les fondements ensemblistes sur lesquels repose l'ensemble des mathématiques discrètes. Nous y étudions les ensembles et leurs opérations, les relations et leurs propriétés, puis les fonctions et la notion de cardinalité.

3.1 Ensembles : notations et opérations fondamentales

3.1.1 Notions de base

Définition 3.1 (Ensemble)**.** Un **ensemble** est une collection d'objets distincts, appelés **éléments**. On note $x \in A$ pour signifier que x est un élément de l'ensemble A, et $x \notin A$ dans le cas contraire.

Notation 3.2. Les ensembles classiques sont notés :

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

L'ensemble vide est noté $\varnothing$ ou $\{\}$.

On décrit un ensemble soit en *extension*, soit en *compréhension* :

— **Extension :** $A = \{2, 3, 5, 7, 11\}$.

— **Compréhension :** $A = \{p \in \mathbb{N} \mid p \text{ est premier et } p \leq 11\}$.

Définition 3.3 (Inclusion, égalité)**.** Soient A et B deux ensembles.

1. $A \subseteq B$ (A **est inclus dans** B) si tout élément de A est élément de B :
$$A \subseteq B \iff \big(\forall x,\ x \in A \Rightarrow x \in B\big).$$
2. $A = B$ si et seulement si $A \subseteq B$ et $B \subseteq A$.
3. $A \subsetneq B$ (**inclusion stricte**) si $A \subseteq B$ et $A \neq B$.

Définition 3.4 (Ensemble des parties)**.** L'**ensemble des parties** de A, noté $\mathcal{P}(A)$, est l'ensemble de tous les sous-ensembles de A :

$$\mathcal{P}(A) = \{B \mid B \subseteq A\}.$$

Exemple 3.5 (Parties d'un petit ensemble)**.** Si $A = \{1, 2, 3\}$, alors

$$\mathcal{P}(A) = \big\{\varnothing, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\big\}.$$

On observe que $\operatorname{card} \mathcal{P}(A) = 2^{\operatorname{card} A} = 2^3 = 8$.

Définition 3.6 (Produit cartésien)**.** Le **produit cartésien** de A et B est

$$A \times B = \{(a, b) \mid a \in A,\ b \in B\}.$$

Plus généralement, $A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in A_i \text{ pour tout } i\}$.

3.1.2 Opérations ensemblistes

Soit Ω un ensemble de référence (univers).

Définition 3.7 (Opérations sur les ensembles)**.** Soient $A, B \subseteq \Omega$.

1. **Union :** $A \cup B = \{x \in \Omega \mid x \in A \text{ ou } x \in B\}$.
2. **Intersection :** $A \cap B = \{x \in \Omega \mid x \in A \text{ et } x \in B\}$.
3. **Complément :** $\overline{A} = A^c = \{x \in \Omega \mid x \notin A\}$.
4. **Différence :** $A \setminus B = \{x \in A \mid x \notin B\}$.
5. **Différence symétrique :** $A \triangle B = (A \setminus B) \cup (B \setminus A)$.

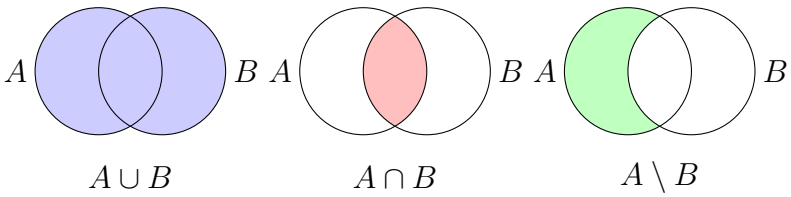


FIGURE 3.1 – Diagrammes de Venn : union, intersection, différence.

Théorème 3.8 (Lois de De Morgan pour les ensembles)**.** *Soient $A, B \subseteq \Omega$. Alors :*

1. $\overline{A \cup B} = \overline{A} \cap \overline{B}$,
2. $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

Démonstration. Montrons (1) par double inclusion.

($\subseteq$) Soit $x \in \overline{A \cup B}$. Alors $x \notin A \cup B$, donc $x \notin A$ *et* $x \notin B$. Par conséquent $x \in \overline{A}$ et $x \in \overline{B}$, d'où $x \in \overline{A} \cap \overline{B}$.

($\supseteq$) Soit $x \in \overline{A} \cap \overline{B}$. Alors $x \notin A$ et $x \notin B$, donc $x \notin A \cup B$, c'est-à-dire $x \in \overline{A \cup B}$.

La preuve de (2) est analogue (ou s'obtient en appliquant (1) à $\overline{A}$ et $\overline{B}$, puis en simplifiant). □

Remarque 3.9 (Paradoxe de Russell). La notion naïve d'ensemble conduit à des contradictions. Considérons l'« ensemble » $R = \{X \mid X \notin X\}$. Si $R \in R$, alors par définition $R \notin R$; si $R \notin R$, alors $R \in R$. Cette contradiction, découverte par Bertrand Russell en 1901, a motivé l'axiomatisation de la théorie des ensembles (par exemple les axiomes de Zermelo–Fraenkel).

3.2 Relations

Définition 3.10 (Relation binaire)**.** Une **relation binaire** de A vers B est un sous-ensemble $\mathcal{R} \subseteq A \times B$. Si $A = B$, on dit que $\mathcal{R}$ est une relation *sur* A. On écrit $a \mathcal{R} b$ au lieu de $(a, b) \in \mathcal{R}$.

Définition 3.11 (Propriétés d'une relation sur A)**.** Soit $\mathcal{R}$ une relation sur A.

1. **Réflexive :** $\forall a \in A,\ a \mathcal{R} a$.
2. **Symétrique :** $\forall a, b \in A,\ a \mathcal{R} b \Rightarrow b \mathcal{R} a$.
3. **Antisymétrique :** $\forall a, b \in A,\ \big(a \mathcal{R} b \text{ et } b \mathcal{R} a\big) \Rightarrow a = b$.
4. **Transitive :** $\forall a, b, c \in A,\ \big(a \mathcal{R} b \text{ et } b \mathcal{R} c\big) \Rightarrow a \mathcal{R} c$.

3.2.1 Relations d'équivalence

Définition 3.12 (Relation d'équivalence)**.** Une relation $\sim$ sur A est une **relation d'équivalence** si elle est réflexive, symétrique et transitive.

Définition 3.13 (Classe d'équivalence)**.** Si $\sim$ est une relation d'équivalence sur A et $a \in A$, la **classe d'équivalence** de a est

$$[a] = \{x \in A \mid x \sim a\}.$$

L'ensemble des classes d'équivalence, noté $A/\!\sim$, est appelé **ensemble quotient**.

Exemple 3.14 (Congruence modulo n)**.** Sur $\mathbb{Z}$, la relation $a \equiv b \pmod{n}$ est une relation d'équivalence. Les classes sont $[0], [1], \ldots, [n-1]$ et l'ensemble quotient est $\mathbb{Z}/n\mathbb{Z}$.

Définition 3.15 (Partition)**.** Une **partition** d'un ensemble A est une famille $\{A_i\}_{i \in I}$ de sous-ensembles non vides de A tels que :

1. $\bigcup_{i \in I} A_i = A$,
2. $A_i \cap A_j = \varnothing$ pour tous $i \neq j$.

Théorème 3.16 (Correspondance équivalence–partition)**.** *Soit A un ensemble non vide. Il y a une correspondance bijective entre les relations d'équivalence sur A et les partitions de A : les classes d'équivalence d'une relation d'équivalence forment une partition, et réciproquement toute partition induit une relation d'équivalence.*

Démonstration. **(Équivalence ⇒ Partition).** Soit $\sim$ une relation d'équivalence sur A. Montrons que $\{[a] \mid a \in A\}$ est une partition.

— *Non-vacuité.* Pour tout $a \in A$, on a $a \in [a]$ (réflexivité), donc $[a] \neq \varnothing$.

— *Recouvrement.* Comme $a \in [a]$ pour tout a, on a $A = \bigcup_{a \in A} [a]$.

— *Disjonction.* Supposons $[a] \cap [b] \neq \varnothing$ et montrons $[a] = [b]$. Soit $c \in [a] \cap [b]$, donc $c \sim a$ et $c \sim b$. Soit $x \in [a]$; alors $x \sim a$. Par symétrie, $a \sim c$; par transitivité, $x \sim c$; puis $c \sim b$ donne $x \sim b$, donc $x \in [b]$. Ainsi $[a] \subseteq [b]$. Par symétrie, $[b] \subseteq [a]$.

(Partition ⇒ Équivalence). Soit $\{A_i\}_{i \in I}$ une partition de A. Définissons $a \sim b$ si et seulement s'il existe $i \in I$ tel que $a, b \in A_i$. On vérifie aisément que $\sim$ est réflexive (car a appartient à un certain A_i), symétrique (par symétrie de la définition) et transitive (si $a, b \in A_i$ et $b, c \in A_j$, alors $b \in A_i \cap A_j$, d'où $i = j$ par disjonction, et donc $a, c \in A_i$). □

3.2.2 Ordres partiels et diagrammes de Hasse

Définition 3.17 (Ordre partiel)**.** Une relation $\preceq$ sur A est un **ordre partiel** si elle est réflexive, antisymétrique et transitive. Le couple $(A, \preceq)$ est un **ensemble partiellement ordonné** (ou **poset**).

Définition 3.18 (Chaîne, antichaîne)**.** Dans un poset $(A, \preceq)$:

— une **chaîne** est un sous-ensemble $C \subseteq A$ tel que deux éléments quelconques de C sont comparables ;

— une **antichaîne** est un sous-ensemble $S \subseteq A$ tel que deux éléments distincts quelconques de S sont incomparables.

Exemple 3.19 (Divisibilité)**.** Sur $A = \{1, 2, 3, 4, 6, 12\}$, la relation $a \mid b$ est un ordre partiel. Le diagramme de Hasse correspondant est donné à la figure 3.2.

Remarque 3.20. Dans un diagramme de Hasse, on ne trace que les relations de *couverture* : a couvre b si $b \prec a$ et il n'existe aucun c avec $b \prec c \prec a$. Les relations déduites par réflexivité et transitivité sont omises.

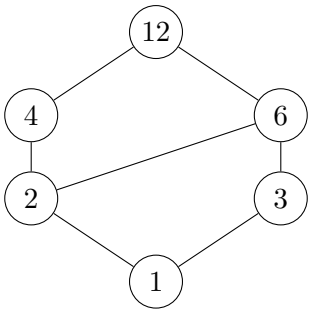


FIGURE 3.2 – Diagramme de Hasse de $(\{1, 2, 3, 4, 6, 12\}, |)$.

Définition 3.21 (Éléments remarquables d'un poset)**.** Soit $(A, \preceq)$ un poset et $S \subseteq A$.

- Un **élément minimal** de S est un $a \in S$ tel qu'il n'existe aucun $b \in S$ avec $b \prec a$.
- Un **minimum** de S est un $a \in S$ tel que $a \preceq b$ pour tout $b \in S$ (s'il existe, il est unique).
- La **borne supérieure** (ou *supremum*) de S, notée $\sup S$, est le plus petit majorant de S.
- La **borne inférieure** (ou *infimum*) de S, notée $\inf S$, est le plus grand minorant de S.

Exemple 3.22 (Poset $(\mathcal{P}(\{a, b\}), \subseteq)$)**.**

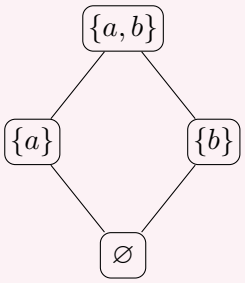


FIGURE 3.3 – Diagramme de Hasse de $(\mathcal{P}(\{a, b\}), \subseteq)$.

Ce poset possède un minimum ($\varnothing$) et un maximum ($\{a, b\}$). Les éléments $\{a\}$ et $\{b\}$ forment une antichaîne.

Théorème 3.23 (Dilworth)**.** *Dans un poset fini, la taille maximale d'une antichaîne est égale au nombre minimal de chaînes nécessaires pour partitionner le poset.*

3.3 Fonctions

Définition 3.24 (Fonction)**.** Une **fonction** $f : A \to B$ est une relation $f \subseteq A \times B$ telle que pour tout $a \in A$, il existe un unique $b \in B$ avec $(a, b) \in f$. L'ensemble A est le **domaine**, B le **codomaine**.

Définition 3.25 (Injection, surjection, bijection)**.** Soit $f\colon A \to B$.

1. f est **injective** si $\forall a_1, a_2 \in A,\ f(a_1) = f(a_2) \Rightarrow a_1 = a_2$.
2. f est **surjective** si $\forall b \in B,\ \exists\, a \in A,\ f(a) = b$.
3. f est **bijective** si elle est à la fois injective et surjective.

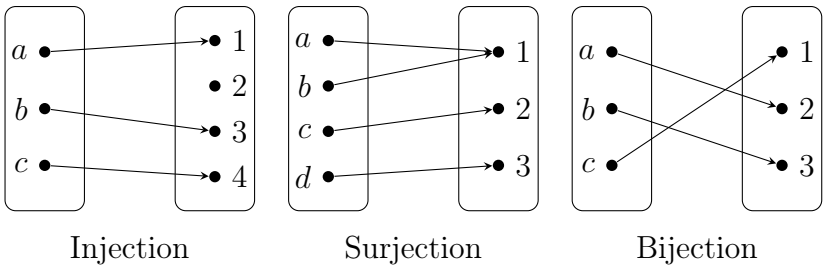


FIGURE 3.4 – Illustration de l'injection, la surjection et la bijection.

Définition 3.26 (Composition)**.** Si $f\colon A \to B$ et $g\colon B \to C$, la **composée** $g \circ f\colon A \to C$ est définie par $(g \circ f)(a) = g\big(f(a)\big)$.

Proposition 3.27 (Composition et injectivité/surjectivité)**.**

1. *Si f et g sont injectives, alors $g \circ f$ est injective.*
2. *Si f et g sont surjectives, alors $g \circ f$ est surjective.*
3. *Si $g \circ f$ est injective, alors f est injective.*
4. *Si $g \circ f$ est surjective, alors g est surjective.*

Démonstration. (1) Supposons $g(f(a_1)) = g(f(a_2))$. L'injectivité de g donne $f(a_1) = f(a_2)$, puis celle de f donne $a_1 = a_2$.

(3) Supposons $f(a_1) = f(a_2)$. Alors $g(f(a_1)) = g(f(a_2))$, et l'injectivité de $g \circ f$ donne $a_1 = a_2$. Les preuves de (2) et (4) sont laissées en exercice. □

Définition 3.28 (Fonction inverse)**.** Si $f\colon A \to B$ est bijective, il existe une unique fonction $f^{-1}\colon B \to A$ telle que $f^{-1} \circ f = \mathrm{id}_A$ et $f \circ f^{-1} = \mathrm{id}_B$.

3.4 Cardinalité

Définition 3.29 (Équipotence)**.** Deux ensembles A et B sont **équipotents** (ont même cardinalité), noté $\operatorname{card} A = \operatorname{card} B$, s'il existe une bijection $f\colon A \to B$.

Définition 3.30 (Ensemble dénombrable)**.** Un ensemble A est **dénombrable** s'il est fini ou s'il existe une bijection $f\colon \mathbb{N} \to A$. Un ensemble qui n'est pas dénombrable est dit **indénombrable**.

Exemple 3.31. L'ensemble $\mathbb{Z}$ est dénombrable. La bijection $f\colon \mathbb{N} \to \mathbb{Z}$ peut être définie par :

$$f(n) = \begin{cases} n/2 & \text{si } n \text{ est pair,} \\ -(n+1)/2 & \text{si } n \text{ est impair.} \end{cases}$$

Ainsi $f(0) = 0,\ f(1) = -1,\ f(2) = 1,\ f(3) = -2,\ f(4) = 2,\ \ldots$

Théorème 3.32 (Cantor : indénombrabilité de $\mathbb{R}$)**.** *L'ensemble $\mathbb{R}$ est indénombrable. Plus précisément, l'intervalle $]0,1[$ n'est pas dénombrable.*

Preuve par l'argument diagonal de Cantor. Supposons par l'absurde qu'il existe une bijection $f\colon \mathbb{N} \to]0,1[$ et écrivons les développements décimaux :

$$f(0) = 0{,}d_{00}\,d_{01}\,d_{02}\ldots, \quad f(1) = 0{,}d_{10}\,d_{11}\,d_{12}\ldots, \quad f(2) = 0{,}d_{20}\,d_{21}\,d_{22}\ldots, \quad \ldots$$

Construisons $x = 0{,}x_0x_1x_2\ldots$ avec

$$x_n = \begin{cases} 3 & \text{si } d_{nn} \neq 3, \\ 7 & \text{si } d_{nn} = 3. \end{cases}$$

On a $x \in]0,1[$ (on évite les chiffres 0 et 9 pour exclure les ambiguïtés de représentation décimale). Or $x \neq f(n)$ pour tout $n \in \mathbb{N}$ car x diffère de $f(n)$ au rang n. Ceci contredit la surjectivité de f. □

Corollaire 3.33. $\operatorname{card}\mathbb{N} < \operatorname{card}\mathcal{P}(\mathbb{N}) = \operatorname{card}\mathbb{R}$.

Théorème 3.34 (Cantor : pas de surjection vers l'ensemble des parties)**.** *Pour tout ensemble A, il n'existe pas de surjection $f\colon A \to \mathcal{P}(A)$. En particulier,* $\operatorname{card} A < \operatorname{card}\mathcal{P}(A)$.

Démonstration. Supposons par l'absurde qu'il existe une surjection $f\colon A \to \mathcal{P}(A)$. Définissons $B = \{a \in A \mid a \notin f(a)\}$. Comme $B \subseteq A$, on a $B \in \mathcal{P}(A)$, donc par surjectivité il existe $b \in A$ tel que $f(b) = B$.

Si $b \in B$, alors par définition de B, on a $b \notin f(b) = B$: contradiction. Si $b \notin B$, alors $b \notin f(b)$, donc par définition de B, on a $b \in B$: contradiction. L'hypothèse est donc absurde. □

Proposition 3.35 (Propriétés de cardinalité)**.**

1. *Si $A \subseteq B$ et B est dénombrable, alors A est dénombrable.*
2. *L'union dénombrable d'ensembles dénombrables est dénombrable.*
3. *Le produit cartésien de deux ensembles dénombrables est dénombrable.*
4. *L'ensemble $\{0,1\}^{\mathbb{N}}$ (suites binaires infinies) est indénombrable et a la même cardinalité que $\mathbb{R}$.*

Exemple 3.36 (Nombres algébriques vs transcendants)**.** L'ensemble des nombres algébriques (racines de polynômes à coefficients entiers) est dénombrable, car il est réunion dénombrable d'ensembles finis. Par conséquent, l'ensemble des nombres transcendants est indénombrable — un argument d'existence non constructif remarquable.

3.5 Exercices

Exercice 3.1 (Opérations ensemblistes)**.** Soient $A = \{1, 2, 3, 4, 5\}$, $B = \{3, 4, 5, 6, 7\}$ et $\Omega = \{1, 2, \ldots, 10\}$. Calculer $A \cup B$, $A \cap B$, $A \setminus B$, $\overline{A}$, $A \triangle B$ et vérifier les lois de De Morgan.

Exercice 3.2 (Ensemble des parties)**.** Montrer par récurrence que $\operatorname{card} \mathcal{P}(A) = 2^{\operatorname{card} A}$ pour tout ensemble fini A.

Exercice 3.3 (Relation d'équivalence)**.** Sur $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$, on définit $(a, b) \sim (c, d)$ si et seulement si $ad = bc$. Montrer que $\sim$ est une relation d'équivalence et interpréter les classes.

Exercice 3.4 (Composition de fonctions)**.** Montrer les points (2) et (4) de la proposition 3.27.

Exercice 3.5 (Dénombrabilité de $\mathbb{Q}$)**.** Montrer que $\mathbb{Q}$ est dénombrable en utilisant un argument de diagonale de Cantor (parcours en zigzag de $\mathbb{N} \times \mathbb{N}^*$).

Exercice 3.6 (Théorème de Cantor)**.** Montrer que pour tout ensemble A (fini ou infini), il n'existe pas de surjection $f \colon A \to \mathcal{P}(A)$. *Indication : considérer* $B = \{a \in A \mid a \notin f(a)\}$.

Exercice 3.7 (Diagramme de Hasse)**.** Dessiner le diagramme de Hasse de $(\mathcal{P}(\{a, b, c\}), \subseteq)$. Identifier les chaînes maximales et les antichaînes maximales.

Exercice 3.8 (Schröder–Bernstein)**.** En admettant le théorème de Cantor–Bernstein (s'il existe une injection de A dans B et une injection de B dans A, alors il existe une bijection entre A et B), montrer que $\operatorname{card}]0, 1[= \operatorname{card} \mathbb{R}$.

Résumé du chapitre 3

- Un **ensemble** est caractérisé par ses éléments ; l'ensemble des parties $\mathcal{P}(A)$ a $2^{\operatorname{card} A}$ éléments.
- Les lois de **De Morgan** relient union, intersection et complémentaire.
- Une **relation d'équivalence** (réflexive, symétrique, transitive) partitionne son ensemble en classes d'équivalence.
- Un **ordre partiel** (réflexif, antisymétrique, transitif) se visualise par un diagramme de Hasse.
- Une fonction est **bijective** si et seulement si elle admet un inverse.
- L'argument diagonal de **Cantor** montre que $\mathbb{R}$ est indénombrable : $\operatorname{card} \mathbb{N} < \operatorname{card} \mathbb{R}$.

Chapitre 4

Combinatoire — Dénombrement

« L'art de compter est l'art de ne compter qu'une fois. »

Le dénombrement — l'art de compter le nombre d'éléments d'un ensemble fini — est une compétence fondamentale en mathématiques discrètes, en informatique et en probabilités. Ce chapitre développe les techniques classiques de combinatoire.

4.1 Principes fondamentaux du dénombrement

Théorème 4.1 (Principe d'addition)**.** *Si $A_1, A_2, \ldots, A_k$ sont des ensembles finis* deux à deux disjoints*, alors*

$$\operatorname{card} A_1 \cup A_2 \cup \cdots \cup A_k = \operatorname{card} A_1 + \operatorname{card} A_2 + \cdots + \operatorname{card} A_k.$$

Démonstration. Par récurrence sur k. Pour $k = 1$, c'est trivial. Si le résultat vaut pour $k-1$ ensembles, alors $\operatorname{card} A_1 \cup \cdots \cup A_k = \operatorname{card}(A_1 \cup \cdots \cup A_{k-1}) \cup A_k$. Comme A_k est disjoint de $A_1 \cup \cdots \cup A_{k-1}$, on obtient $\operatorname{card} A_1 \cup \cdots \cup A_{k-1} + \operatorname{card} A_k$, et on conclut par hypothèse de récurrence. □

Théorème 4.2 (Principe de multiplication)**.** *Si une procédure se décompose en k étapes successives, la i-ème étape pouvant être réalisée de n_i façons (indépendamment des choix précédents), alors le nombre total de réalisations est $n_1 \cdot n_2 \cdots n_k$. Formellement :*

$$\operatorname{card} A_1 \times A_2 \times \cdots \times A_k = \operatorname{card} A_1 \cdot \operatorname{card} A_2 \cdots \operatorname{card} A_k.$$

Démonstration. Par récurrence sur k. Pour $k = 1$, c'est trivial. Supposons le résultat vrai pour $k-1$ ensembles. On peut écrire $A_1 \times \cdots \times A_k = (A_1 \times \cdots \times A_{k-1}) \times A_k$. Pour chacun des $\operatorname{card} A_1 \cdots \operatorname{card} A_{k-1}$ éléments du premier facteur (par hypothèse de récurrence), il y a $\operatorname{card} A_k$ choix pour la dernière composante, d'où le résultat. □

Exemple 4.3 (Plaques d'immatriculation)**.** Une plaque est composée de 2 lettres suivies de 3 chiffres puis de 2 lettres (format AA-000-AA). Le nombre de plaques possibles est $26^2 \cdot 10^3 \cdot 26^2 = 26^4 \cdot 10^3 = 456\,976 \cdot 1000 = 456\,976\,000$.

4.2 Permutations et arrangements

Définition 4.4 (Factorielle)**.** Pour $n \in \mathbb{N}$, la **factorielle** de n est

$$n! = \begin{cases} 1 & \text{si } n = 0, \\ n \cdot (n-1)! & \text{si } n \geq 1. \end{cases}$$

Définition 4.5 (Permutation)**.** Une **permutation** d'un ensemble à n éléments est un arrangement ordonné de *tous* ses éléments. Le nombre de permutations est $n!$.

Définition 4.6 (Arrangement (permutation partielle))**.** Le nombre de façons de choisir k éléments *ordonnés* parmi n est

$$A(n,k) = \frac{n!}{(n-k)!} = n(n-1)\cdots(n-k+1).$$

Exemple 4.7. Lors d'une course de 10 athlètes, le nombre de podiums possibles (or, argent, bronze) est $A(10,3) = 10 \cdot 9 \cdot 8 = 720$.

4.3 Combinaisons et coefficients binomiaux

Définition 4.8 (Combinaison, coefficient binomial)**.** Le nombre de sous-ensembles à k éléments d'un ensemble à n éléments est le **coefficient binomial**

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!}, \quad 0 \leq k \leq n.$$

Par convention, $\binom{n}{k} = 0$ si $k < 0$ ou $k > n$.

Exemple 4.9 (Calculs de coefficients binomiaux)**.**

$$\binom{10}{3} = \frac{10!}{3!\,7!} = \frac{10 \cdot 9 \cdot 8}{3 \cdot 2 \cdot 1} = 120, \qquad \binom{8}{5} = \binom{8}{3} = \frac{8 \cdot 7 \cdot 6}{6} = 56.$$

Proposition 4.10 (Propriétés élémentaires)**.**

1. *Symétrie :* $\binom{n}{k} = \binom{n}{n-k}$.
2. *Bords :* $\binom{n}{0} = \binom{n}{n} = 1$.
3. *Formule de Pascal :* $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$ *pour* $1 \leq k \leq n-1$.

Démonstration. (3) On interprète combinatoirement. Parmi les $\binom{n}{k}$ sous-ensembles de $\{1,\dots,n\}$ à k éléments, ceux contenant n sont au nombre de $\binom{n-1}{k-1}$ (on choisit les $k-1$ restants parmi $\{1,\dots,n-1\}$) et ceux ne contenant pas n sont au nombre de $\binom{n-1}{k}$. □

4.3.1 Triangle de Pascal

$$
\begin{array}{ccccccccccccc}
 & & & & & & 1 & & & & & & \\
 & & & & & 1 & & 1 & & & & & \\
 & & & & 1 & & 2 & & 1 & & & & \\
 & & & 1 & & 3 & & 3 & & 1 & & & \\
 & & 1 & & 4 & & 6 & & 4 & & 1 & & \\
 & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & \\
1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 \\
1 & & 7 & & 21 & & 35 & & 35 & & 21 & & 7 & & 1
\end{array}
$$

FIGURE 4.1 – Les huit premières lignes du triangle de Pascal ($n = 0, 1, \dots, 7$).

4.4 Théorème binomial

Théorème 4.11 (Théorème binomial (binôme de Newton))**.** *Pour tous a, b et tout $n \in \mathbb{N}$:*

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

Preuve par récurrence. **Base.** Pour $n = 0$: $(a+b)^0 = 1 = \binom{0}{0} a^0 b^0$. ✓

Hérédité. Supposons la formule vraie au rang n. Alors :

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)\sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k \\
&= \sum_{k=0}^{n}\binom{n}{k}a^{n+1-k}b^k + \sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^{k+1} \\
&= \sum_{k=0}^{n}\binom{n}{k}a^{n+1-k}b^k + \sum_{j=1}^{n+1}\binom{n}{j-1}a^{n+1-j}b^j \quad (j=k+1) \\
&= a^{n+1} + \sum_{k=1}^{n}\left[\binom{n}{k}+\binom{n}{k-1}\right]a^{n+1-k}b^k + b^{n+1} \\
&= a^{n+1} + \sum_{k=1}^{n}\binom{n+1}{k}a^{n+1-k}b^k + b^{n+1} \quad \text{(Pascal)} \\
&= \sum_{k=0}^{n+1}\binom{n+1}{k}a^{n+1-k}b^k.
\end{aligned}$$

□

Corollaire 4.12. *En posant $a=b=1$:* $\displaystyle\sum_{k=0}^{n}\binom{n}{k}=2^n$. *En posant $a=1$, $b=-1$:* $\displaystyle\sum_{k=0}^{n}(-1)^k\binom{n}{k}=0$.

4.5 Identité de Vandermonde

Théorème 4.13 (Identité de Vandermonde)**.** *Pour tous entiers $m,n,r\geq 0$:*

$$\binom{m+n}{r}=\sum_{k=0}^{r}\binom{m}{k}\binom{n}{r-k}.$$

Preuve combinatoire. Considérons un ensemble de $m+n$ personnes, divisé en un groupe A de m personnes et un groupe B de n personnes. Le nombre de façons de choisir r personnes parmi $m+n$ est $\binom{m+n}{r}$.

D'autre part, si l'on choisit exactement k personnes dans A et $r-k$ dans B, cela peut se faire de $\binom{m}{k}\binom{n}{r-k}$ façons. En sommant sur toutes les valeurs possibles de k (de 0 à r), on obtient le membre de droite. □

Corollaire 4.14. *En posant $m=n=r$:* $\displaystyle\sum_{k=0}^{n}\binom{n}{k}^2=\binom{2n}{n}$.

4.6 Combinaisons avec répétition

Définition 4.15 (Combinaison avec répétition)**.** Le nombre de façons de choisir k éléments parmi n types *avec répétition autorisée* (l'ordre ne comptant pas) est le **coefficient multiensemble** :

$$\left(\!\binom{n}{k}\!\right) = \binom{n+k-1}{k} = \binom{n+k-1}{n-1}.$$

Exemple 4.16 (Boules de glace)**.** Un glacier propose 5 parfums. Le nombre de coupes de 3 boules (avec répétition possible, sans ordre) est

$$\left(\!\binom{5}{3}\!\right) = \binom{5+3-1}{3} = \binom{7}{3} = 35.$$

4.7 Permutations avec répétition et anagrammes

Théorème 4.17 (Permutations avec répétition)**.** *Le nombre de permutations de n objets où l'objet de type i apparaît n_i fois ($n_1 + n_2 + \cdots + n_r = n$) est le* ***coefficient multinomial*** *:*

$$\binom{n}{n_1, n_2, \ldots, n_r} = \frac{n!}{n_1!\, n_2! \cdots n_r!}.$$

Démonstration. Il y a $n!$ façons d'ordonner n objets distincts. Or les $n_i!$ permutations internes des objets de type i produisent le même arrangement. On divise donc par $n_1!\, n_2! \cdots n_r!$. □

Exemple 4.18 (Anagrammes)**.** Le nombre d'anagrammes du mot MISSISSIPPI est :

$$\frac{11!}{1!\,4!\,4!\,2!} = \frac{39\,916\,800}{1 \cdot 24 \cdot 24 \cdot 2} = 34\,650.$$

En effet : M apparaît 1 fois, I 4 fois, S 4 fois, P 2 fois.

4.8 Méthode des boules et barres

Théorème 4.19 (Principe d'inclusion-exclusion)**.** *Pour des ensembles finis $A_1, \ldots, A_n$:*

$$\operatorname{card} A_1 \cup \cdots \cup A_n = \sum_i \operatorname{card} A_i - \sum_{i<j} \operatorname{card} A_i \cap A_j + \sum_{i<j<k} \operatorname{card} A_i \cap A_j \cap A_k - \cdots + (-1)^{n+1} \operatorname{card} A_1 \cap \cdot$$

Démonstration. Montrons que chaque élément $x \in A_1 \cup \cdots \cup A_n$ est compté exactement une fois dans le membre de droite. Supposons que x appartient à exactement m des

ensembles ($m \geq 1$). Sa contribution au membre de droite est

$$\binom{m}{1} - \binom{m}{2} + \binom{m}{3} - \cdots + (-1)^{m+1}\binom{m}{m} = -\sum_{k=0}^{m}(-1)^k\binom{m}{k} + 1 = -(1-1)^m + 1 = 1,$$

par le théorème binomial. Donc chaque élément est compté exactement une fois. □

Exemple 4.20 (Inclusion-exclusion pour deux ensembles)**.** Pour deux ensembles finis : $\operatorname{card} A \cup B = \operatorname{card} A + \operatorname{card} B - \operatorname{card} A \cap B$.

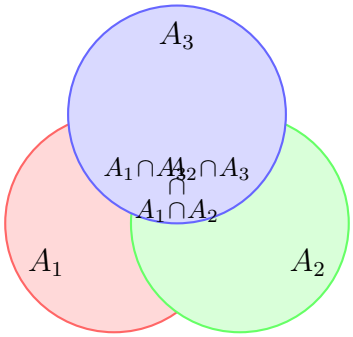


FIGURE 4.2 – Diagramme de Venn pour trois ensembles (inclusion-exclusion).

Théorème 4.21 (Boules et barres (stars and bars))**.** *Le nombre de solutions entières de*

$$x_1 + x_2 + \cdots + x_k = n, \quad x_i \geq 0,$$

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

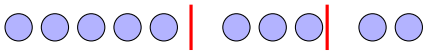
Démonstration. Représentons chaque solution par une suite de n étoiles ($*$) et $k-1$ barres ($|$). Les étoiles avant la première barre représentent x_1, celles entre les barres $i-1$ et i représentent x_i, etc.

Par exemple, pour $k = 3$, $n = 5$, la configuration $**\,|\,*\,|\,**$ correspond à $(x_1, x_2, x_3) = (2, 1, 2)$.

Une telle configuration est une suite de $n + k - 1$ symboles dont $k - 1$ sont des barres. Le nombre de configurations est donc $\binom{n+k-1}{k-1}$. □

Remarque 4.22. Si l'on impose $x_i \geq 1$, le changement de variable $y_i = x_i - 1$ ramène au cas $y_1 + \cdots + y_k = n - k$ avec $y_i \geq 0$, donnant $\binom{n-1}{k-1}$ solutions.

Exemple 4.23. Combien y a-t-il de façons de répartir 10 bonbons identiques entre 4 enfants ? Réponse : $\binom{10+4-1}{4-1} = \binom{13}{3} = 286$.



$$\star\star\star\star\star \mid \star\star\star \mid \star\star \longleftrightarrow (5,3,2)$$

FIGURE 4.3 – Illustration de la méthode des boules et barres pour $n = 10$, $k = 3$.

4.9 Dérangements

Définition 4.24 (Dérangement)**.** Un **dérangement** d'un ensemble $\{1, 2, \ldots, n\}$ est une permutation σ sans point fixe, c'est-à-dire telle que $\sigma(i) \neq i$ pour tout i. Le nombre de dérangements de n éléments est noté D_n (ou $!n$, la **sous-factorielle**).

Théorème 4.25 (Formule des dérangements)**.** *Pour tout $n \geq 0$:*

$$D_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}.$$

En particulier, $D_0 = 1$, $D_1 = 0$, $D_2 = 1$, $D_3 = 2$, $D_4 = 9$, $D_5 = 44$.

Démonstration. Soit A_i l'ensemble des permutations de $\{1, \ldots, n\}$ qui fixent i. Par le principe d'inclusion-exclusion :

$$\begin{aligned} D_n &= n! - \operatorname{card} A_1 \cup A_2 \cup \cdots \cup A_n \\ &= n! - \sum_i \operatorname{card} A_i + \sum_{i<j} \operatorname{card} A_i \cap A_j - \cdots + (-1)^n \operatorname{card} A_1 \cap \cdots \cap A_n. \end{aligned}$$

Or $\operatorname{card} A_{i_1} \cap \cdots \cap A_{i_k} = (n-k)!$ (on fixe les positions $i_1, \ldots, i_k$ et on permute les $n-k$ restantes). Il y a $\binom{n}{k}$ façons de choisir les k indices. Donc :

$$D_n = \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)! = \sum_{k=0}^{n} (-1)^k \frac{n!}{k!} = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}. \qquad \square$$

Remarque 4.26. Comme $\displaystyle\sum_{k=0}^{\infty} \frac{(-1)^k}{k!} = e^{-1}$, on a l'approximation $D_n \approx n!/e$, et plus précisément D_n est l'entier le plus proche de $n!/e$.

Proposition 4.27 (Récurrence pour D_n)**.** *Pour $n \geq 2$:*

$$D_n = (n-1)(D_{n-1} + D_{n-2}).$$

Démonstration. Considérons un dérangement σ de $\{1, \ldots, n\}$. Posons $\sigma(1) = j$ avec $j \neq 1$ (il y a $n-1$ choix pour j). Deux cas :

— Si $\sigma(j) = 1$: les éléments 1 et j s'échangent, et les $n-2$ restants forment un dérangement. Il y a D_{n-2} possibilités.

— Si $\sigma(j) \neq 1$: on peut interpréter la restriction aux éléments $\{2, \ldots, n\}$ comme un dérangement de $n-1$ éléments (en remplaçant la contrainte $\sigma(j) \neq 1$ par $\sigma(j) \neq j$). Il y a D_{n-1} possibilités.

Au total, $D_n = (n-1)(D_{n-1} + D_{n-2})$. □

4.10 Exemples résolus

Exemple 4.28 (Sous-ensembles d'un ensemble)**.** Combien de sous-ensembles de $\{1, 2, \ldots, 10\}$ contiennent exactement 3 éléments pairs et 2 éléments impairs ?
Solution. Il y a 5 nombres pairs $(2, 4, 6, 8, 10)$ et 5 nombres impairs $(1, 3, 5, 7, 9)$. Le nombre de sous-ensembles cherchés est $\binom{5}{3}\binom{5}{2} = 10 \cdot 10 = 100$.

Exemple 4.29 (Diagonales d'un polygone)**.** Un polygone convexe à n sommets possède $\binom{n}{2} - n = \frac{n(n-3)}{2}$ diagonales. En effet, $\binom{n}{2}$ est le nombre total de segments reliant deux sommets, et n d'entre eux sont des côtés.

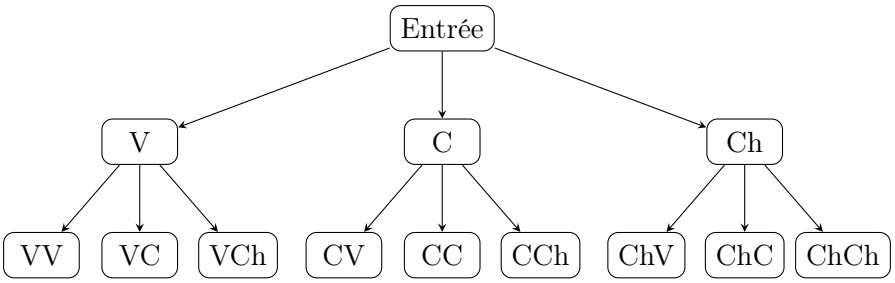


FIGURE 4.4 – Arbre de dénombrement pour un menu à 2 plats choisis parmi viande (V), poisson (C) et champignons (Ch) — principe de multiplication : $3 \times 3 = 9$.

Exemple 4.30 (Comité avec conditions)**.** Dans un groupe de 8 hommes et 6 femmes, on veut former un comité de 5 personnes contenant au moins 2 femmes. Combien de comités possibles ?
Solution. On compte selon le nombre de femmes $f \in \{2, 3, 4, 5\}$:

$$\sum_{f=2}^{5} \binom{6}{f}\binom{8}{5-f} = \binom{6}{2}\binom{8}{3} + \binom{6}{3}\binom{8}{2} + \binom{6}{4}\binom{8}{1} + \binom{6}{5}\binom{8}{0}.$$

Calcul : $15 \cdot 56 + 20 \cdot 28 + 15 \cdot 8 + 6 \cdot 1 = 840 + 560 + 120 + 6 = 1526$.

Exemple 4.31 (Chemins sur une grille)**.** Combien de chemins mènent du point $(0, 0)$ au point (m, n) sur une grille, si l'on ne peut se déplacer que vers la droite (D) ou vers le haut (H) ?
Solution. Chaque chemin est une suite de m pas D et n pas H, soit une suite de $m+n$ pas dont m sont D. Le nombre de chemins est $\binom{m+n}{m}$.
Par exemple, de $(0, 0)$ à $(4, 3)$: $\binom{7}{4} = 35$ chemins.

Exemple 4.32 (Distribution dans des boîtes distinctes)**.** De combien de façons peut-on répartir 12 livres *identiques* en 4 étagères (pouvant être vides) ?
Solution. C'est le problème $x_1 + x_2 + x_3 + x_4 = 12$ avec $x_i \geq 0$. Par la méthode des boules et barres : $\binom{12+4-1}{4-1} = \binom{15}{3} = 455$.

Exemple 4.33 (Mots de passe)**.** Un mot de passe contient exactement 8 caractères choisis parmi 26 lettres minuscules et 10 chiffres. Il doit contenir au moins un chiffre. Combien de mots de passe valides ?
Solution. Total de mots de passe de longueur 8 : 36^8. Ceux sans chiffre : 26^8. Donc le nombre de mots de passe valides est $36^8 - 26^8 = 2\,821\,109\,907\,456 - 208\,827\,064\,576 = 2\,612\,282\,842\,880$.

Exemple 4.34 (Le problème des lettres et enveloppes)**.** On place au hasard 5 lettres dans 5 enveloppes adressées. Quelle est la probabilité qu'aucune lettre ne soit dans la bonne enveloppe ?
Solution. C'est le problème des dérangements. Le nombre de dérangements de 5 éléments est $D_5 = 5!\left(1 - 1 + \frac{1}{2} - \frac{1}{6} + \frac{1}{24} - \frac{1}{120}\right) = 120 \cdot \frac{11}{30} = 44$. La probabilité est $D_5/5! = 44/120 = 11/30 \approx 0{,}367$.

Exemple 4.35 (Fonction surjective)**.** Le nombre de fonctions surjectives de $\{1, \ldots, n\}$ vers $\{1, \ldots, k\}$ $(n \geq k)$ est donné par la formule d'inclusion-exclusion :

$$S(n,k) = \sum_{j=0}^{k} (-1)^j \binom{k}{j} (k-j)^n.$$

Par exemple, le nombre de surjections de $\{1, \ldots, 4\}$ vers $\{1, 2, 3\}$ est

$$\binom{3}{0}3^4 - \binom{3}{1}2^4 + \binom{3}{2}1^4 - \binom{3}{3}0^4 = 81 - 48 + 3 - 0 = 36.$$

4.11 Exercices

Exercice 4.1 (Principes de base)**.**
1. Combien de chaînes binaires de longueur 10 commencent par 11 ou finissent par 00 ?
2. Combien de nombres entre 1 et 1000 sont divisibles par 3 ou par 5 ?

Exercice 4.2 (Permutations)**.** De combien de façons peut-on asseoir 8 personnes autour d'une table ronde (deux dispositions sont identiques si l'on peut passer de l'une à l'autre par rotation) ?

Exercice 4.3 (Identités binomiales)**.** Démontrer les identités suivantes :
1. $\displaystyle\sum_{k=0}^{n} k\binom{n}{k} = n\,2^{n-1}$.
2. $\displaystyle\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}$.

3. $\binom{n}{k}\binom{k}{j} = \binom{n}{j}\binom{n-j}{k-j}$ pour $0 \leq j \leq k \leq n$.

Exercice 4.4 (Anagrammes avec contraintes). 1. Combien d'anagrammes du mot ARRANGEMENT ?

2. Combien d'anagrammes du mot COMBINATOIRE ne commencent pas par une voyelle ?

Exercice 4.5 (Boules et barres). 1. Combien de solutions entières a l'équation $x_1 + x_2 + x_3 + x_4 = 20$ avec $x_i \geq 0$?

2. Même question avec $x_i \geq 2$ pour tout i.

3. Combien de solutions avec $0 \leq x_i \leq 5$? *(Utiliser l'inclusion-exclusion.)*

Exercice 4.6 (Dérangements). 1. Calculer D_6 et D_7 en utilisant la formule de récurrence.

2. Montrer que $D_n = nD_{n-1} + (-1)^n$ pour $n \geq 1$.

3. Soit $p_n = D_n/n!$ la probabilité qu'une permutation aléatoire soit un dérangement. Montrer que $\lim_{n\to\infty} p_n = 1/e$.

Exercice 4.7 (Chemins avec obstacles). Combien de chemins sur grille de $(0,0)$ à $(6,6)$ (pas D et H) passent par le point $(3,3)$?

Exercice 4.8 (Dénombrement avancé). On dispose de n billes *distinctes* et de k boîtes *distinctes*.

1. Combien de répartitions si les boîtes peuvent être vides ?
2. Combien si chaque boîte contient au plus une bille ($n \leq k$) ?
3. Combien si chaque boîte contient au moins une bille ($n \geq k$) ?

Exercice 4.9 (Identité de Vandermonde généralisée). En utilisant le théorème binomial appliqué à $(1+x)^m(1+x)^n = (1+x)^{m+n}$, retrouver l'identité de Vandermonde $\binom{m+n}{r} = \sum_{k=0}^{r} \binom{m}{k}\binom{n}{r-k}$.

Exercice 4.10 (Surjections). 1. Combien de surjections y a-t-il de $\{1,\ldots,5\}$ vers $\{a,b,c\}$?

2. Montrer que le nombre de surjections de $\{1,\ldots,n\}$ vers $\{1,\ldots,n\}$ est $n!$.

Exercice 4.11 (Nombres à chiffres distincts). Combien de nombres de 4 chiffres (entre 1000 et 9999) ont tous leurs chiffres distincts ?

Exercice 4.12 (Problème de Lucas). Combien y a-t-il de façons de choisir k éléments non consécutifs dans $\{1,2,\ldots,n\}$ (disposés en ligne) ? Montrer que la réponse est $\binom{n-k+1}{k}$.

Exercice 4.13 (Problème du chapelier). n personnes déposent leur chapeau au vestiaire. Les chapeaux sont rendus au hasard. Calculer la probabilité qu'au moins une personne reçoive son propre chapeau. *(Utiliser l'inclusion-exclusion et les dérangements.)*

Résumé du chapitre 4

— Les **principes d'addition et de multiplication** sont les outils fondamentaux du dénombrement.

— **Permutations** : $n!$ ordres de n éléments ; **arrangements** : $A(n,k) = n!/(n-k)!$.

— **Combinaisons** : $\binom{n}{k} = \frac{n!}{k!(n-k)!}$; la formule de Pascal donne le triangle du même nom.

— Le **théorème binomial** : $(a+b)^n = \sum_k \binom{n}{k} a^{n-k} b^k$.

— L'**identité de Vandermonde** : $\binom{m+n}{r} = \sum_k \binom{m}{k}\binom{n}{r-k}$.

— **Combinaisons avec répétition** : $\binom{n+k-1}{k}$ choix de k éléments parmi n types.

— **Permutations avec répétition** (multinomiales) : $\frac{n!}{n_1!\cdots n_r!}$.

— La méthode des **boules et barres** résout les équations $x_1 + \cdots + x_k = n$ en entiers non négatifs : $\binom{n+k-1}{k-1}$ solutions.

— Les **dérangements** $D_n = n! \sum_{k=0}^{n} (-1)^k/k!$ comptent les permutations sans point fixe ; $D_n \approx n!/e$.

Chapitre 5

Principe d'Inclusion-Exclusion et Dénombrement Avancé

5.1 Le principe d'inclusion-exclusion

Le principe d'inclusion-exclusion est l'un des outils les plus puissants du dénombrement. Il permet de calculer le cardinal de l'union de plusieurs ensembles à partir des cardinaux de leurs intersections.

5.1.1 Cas de deux ensembles

Théorème 5.1 (Inclusion-exclusion pour deux ensembles)**.** *Soient A et B deux ensembles finis. Alors*

$$\operatorname{card} A \cup B = \operatorname{card} A + \operatorname{card} B - \operatorname{card} A \cap B.$$

Démonstration. Chaque élément x de $A \cup B$ appartient à exactement l'une des trois régions disjointes : $A \setminus B$, $B \setminus A$ ou $A \cap B$. On a donc

$$\operatorname{card} A \cup B = \operatorname{card} A \setminus B + \operatorname{card} B \setminus A + \operatorname{card} A \cap B.$$

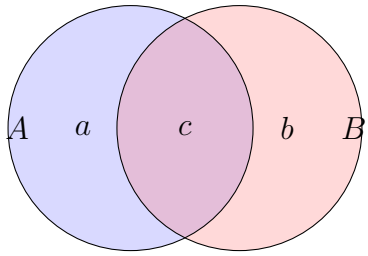
Or $\operatorname{card} A = \operatorname{card} A \setminus B + \operatorname{card} A \cap B$ et $\operatorname{card} B = \operatorname{card} B \setminus A + \operatorname{card} A \cap B$, d'où

$$\operatorname{card} A + \operatorname{card} B = \operatorname{card} A \setminus B + \operatorname{card} B \setminus A + 2 \operatorname{card} A \cap B.$$

En soustrayant $\operatorname{card} A \cap B$, on obtient le résultat. □

Exemple 5.2 (Divisibilité)**.** Combien d'entiers de $\{1, 2, \ldots, 100\}$ sont divisibles par 2 ou par 3 ? Posons $A = \{n \in \{1, \ldots, 100\} : 2 \mid n\}$ et $B = \{n \in \{1, \ldots, 100\} : 3 \mid n\}$. Alors $\operatorname{card} A = 50$, $\operatorname{card} B = 33$ et $\operatorname{card} A \cap B = \lfloor 100/6 \rfloor = 16$. Par inclusion-exclusion,

$$\operatorname{card} A \cup B = 50 + 33 - 16 = 67.$$



$$\operatorname{card} A \cup B = a + b + c = \operatorname{card} A + \operatorname{card} B - \operatorname{card} A \cap B$$

FIGURE 5.1 – Diagramme de Venn pour deux ensembles : $a = \operatorname{card} A \setminus B$, $b = \operatorname{card} B \setminus A$, $c = \operatorname{card} A \cap B$.

5.1.2 Cas de trois ensembles

Théorème 5.3 (Inclusion-exclusion pour trois ensembles)**.** *Soient A, B et C trois ensembles finis. Alors*

$$\operatorname{card} A \cup B \cup C = \operatorname{card} A + \operatorname{card} B + \operatorname{card} C - \operatorname{card} A \cap B - \operatorname{card} A \cap C - \operatorname{card} B \cap C + \operatorname{card} A \cap B \cap C.$$

Démonstration. Appliquons le théorème 5.1 à $A \cup B$ et C :

$$\operatorname{card} (A \cup B) \cup C = \operatorname{card} A \cup B + \operatorname{card} C - \operatorname{card} (A \cup B) \cap C.$$

Or $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$, donc

$$\operatorname{card} (A \cup B) \cap C = \operatorname{card} A \cap C + \operatorname{card} B \cap C - \operatorname{card} A \cap B \cap C.$$

En combinant avec $\operatorname{card} A \cup B = \operatorname{card} A + \operatorname{card} B - \operatorname{card} A \cap B$, on obtient la formule annoncée. □

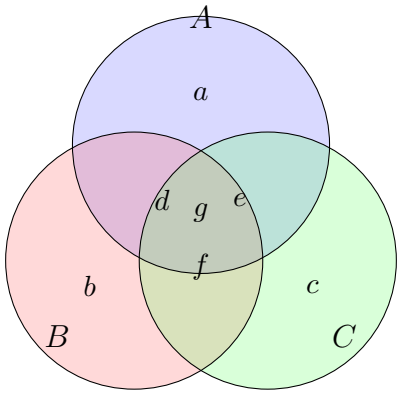


FIGURE 5.2 – Diagramme de Venn pour trois ensembles. Les sept régions correspondent aux différentes intersections.

Exemple 5.4 (Langues parlées)**.** Dans une classe de 100 étudiants, 60 parlent anglais, 45 parlent espagnol et 35 parlent allemand. De plus, 20 parlent anglais et espagnol, 15 parlent anglais et allemand, 12 parlent espagnol et allemand, et 5 parlent les trois

langues. Combien d'étudiants parlent au moins une de ces langues ?
Par inclusion-exclusion :

$$\operatorname{card} A \cup E \cup G = 60 + 45 + 35 - 20 - 15 - 12 + 5 = 98.$$

Ainsi, 2 étudiants ne parlent aucune de ces trois langues.

5.1.3 Le cas général

Théorème 5.5 (Principe d'inclusion-exclusion général)**.** *Soient $A_1, A_2, \ldots, A_n$ des ensembles finis. Alors*

$$\operatorname{card} *\bigcup_{i=1}^{n} A_i = \sum_{k=1}^{n} (-1)^{k+1} \sum_{1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant n} \operatorname{card} A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}.$$

Démonstration. Montrons que chaque élément $x \in \bigcup_{i=1}^{n} A_i$ est compté exactement une fois dans le membre de droite. Supposons que x appartient à exactement m ensembles parmi $A_1, \ldots, A_n$, avec $m \geqslant 1$. L'élément x contribue au terme d'indice k exactement $\binom{m}{k}$ fois (il faut choisir k ensembles parmi les m qui le contiennent). Sa contribution totale est

$$\sum_{k=1}^{m} (-1)^{k+1} \binom{m}{k} = -\sum_{k=1}^{m} (-1)^{k} \binom{m}{k} = -\left[\sum_{k=0}^{m} (-1)^{k} \binom{m}{k} - 1 \right] = -(0 - 1) = 1,$$

car $\sum_{k=0}^{m} (-1)^k \binom{m}{k} = (1-1)^m = 0$ pour $m \geqslant 1$ d'après le binôme de Newton. □

Remarque 5.6. Le principe s'écrit souvent sous la forme complémentaire. Si tous les A_i sont des sous-ensembles d'un univers fini U, alors le nombre d'éléments n'appartenant à *aucun* des A_i est

$$\operatorname{card} *U \setminus \bigcup_{i=1}^{n} A_i = \operatorname{card} U - \sum_{k=1}^{n} (-1)^{k+1} \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} \operatorname{card} A_{i_1} \cap \cdots \cap A_{i_k}.$$

C'est cette forme que l'on utilise le plus souvent en pratique.

5.2 Applications du principe d'inclusion-exclusion

5.2.1 Dénombrement des surjections

Théorème 5.7 (Nombre de surjections)**.** *Le nombre de surjections d'un ensemble à n éléments vers un ensemble à k éléments (avec $n \geqslant k$) est*

$$S(n,k) = \sum_{j=0}^{k} (-1)^j \binom{k}{j} (k-j)^n.$$

Démonstration. Soit $B = \{b_1, \dots, b_k\}$ l'ensemble d'arrivée. Pour chaque i, posons $A_i = \{f : \{1, \dots, n\} \to B \mid b_i \notin \mathrm{Im}(f)\}$, l'ensemble des fonctions qui « évitent » b_i. Une fonction f est surjective si et seulement si elle n'appartient à aucun A_i. Par inclusion-exclusion (forme complémentaire),

$$\begin{aligned} S(n,k) &= k^n - \operatorname{card} * \bigcup_{i=1}^{k} A_i \\ &= \sum_{j=0}^{k} (-1)^j \binom{k}{j} (k-j)^n, \end{aligned}$$

car l'intersection $A_{i_1} \cap \cdots \cap A_{i_j}$ consiste en les fonctions évitant j éléments fixés, donc à valeurs dans un ensemble de $k-j$ éléments, et $\operatorname{card} A_{i_1} \cap \cdots \cap A_{i_j} = (k-j)^n$. □

Exemple 5.8. Le nombre de surjections de $\{1,2,3,4\}$ vers $\{a,b,c\}$ est

$$S(4,3) = \binom{3}{0}3^4 - \binom{3}{1}2^4 + \binom{3}{2}1^4 - \binom{3}{3}0^4 = 81 - 48 + 3 - 0 = 36.$$

5.2.2 L'indicatrice d'Euler via inclusion-exclusion

Définition 5.9 (Indicatrice d'Euler)**.** Pour $n \geqslant 1$, l'indicatrice d'Euler $\varphi(n)$ est le nombre d'entiers k tels que $1 \leqslant k \leqslant n$ et $\mathrm{pgcd}(k,n) = 1$.

Théorème 5.10 (Formule d'Euler via inclusion-exclusion)**.** *Si $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ est la factorisation en nombres premiers de n, alors*

$$\varphi(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

Démonstration. Soit $U = \{1, 2, \dots, n\}$ et pour chaque i, posons $A_i = \{k \in U : p_i \mid k\}$. Un entier $k \in U$ satisfait $\mathrm{pgcd}(k,n) > 1$ si et seulement si $k \in A_i$ pour au moins un i. Donc $\varphi(n) = \operatorname{card} U \setminus \bigcup_{i=1}^{r} A_i$.

On a $\operatorname{card} A_i = n/p_i$, et plus généralement, pour $1 \leqslant i_1 < \cdots < i_s \leqslant r$:

$$\operatorname{card} A_{i_1} \cap \cdots \cap A_{i_s} = \frac{n}{p_{i_1} \cdots p_{i_s}}.$$

Par inclusion-exclusion,

$$\begin{aligned} \varphi(n) &= n - \sum_i \frac{n}{p_i} + \sum_{i<j} \frac{n}{p_i p_j} - \cdots + (-1)^r \frac{n}{p_1 \cdots p_r} \\ &= n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right). \end{aligned}$$

□

Exemple 5.11. Calculons $\varphi(360)$. Puisque $360 = 2^3 \cdot 3^2 \cdot 5$,

$$\varphi(360) = 360 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 360 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 96.$$

5.2.3 Les dérangements

Définition 5.12 (Dérangement)**.** Un *dérangement* de $\{1, 2, \ldots, n\}$ est une permutation σ telle que $\sigma(i) \neq i$ pour tout i. On note D_n le nombre de dérangements de $\{1, \ldots, n\}$.

Théorème 5.13 (Formule des dérangements)**.** *Pour tout $n \geqslant 0$,*

$$D_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}.$$

En particulier, D_n est l'entier le plus proche de $n!/e$.

Démonstration. Soit $A_i = \{\sigma \in \mathfrak{S}_n : \sigma(i) = i\}$ l'ensemble des permutations fixant i. Un dérangement est une permutation n'appartenant à aucun A_i, donc

$$D_n = n! - \operatorname{card} * \bigcup_{i=1}^{n} A_i.$$

Pour tout sous-ensemble $\{i_1, \ldots, i_k\}$, $\operatorname{card} A_{i_1} \cap \cdots \cap A_{i_k} = (n-k)!$ (les k éléments sont fixés, les $n-k$ restants permutent librement). Il y a $\binom{n}{k}$ tels sous-ensembles, d'où par inclusion-exclusion :

$$D_n = \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)! = \sum_{k=0}^{n} (-1)^k \frac{n!}{k!} = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}. \qquad \square$$

Exemple 5.14 (Premières valeurs)**.**

n	0	1	2	3	4	5	6	7
D_n	1	0	1	2	9	44	265	1 854
$D_n/n!$	1	0	0,5	0,333	0,375	0,367	0,368	0,368

On observe que $D_n/n! \to 1/e \approx 0{,}3679$.

Corollaire 5.15 (Récurrence des dérangements)**.** *Pour $n \geqslant 2$, on a $D_n = (n-1)(D_{n-1} + D_{n-2})$.*

Démonstration. Soit σ un dérangement de $\{1, \ldots, n\}$. Posons $\sigma(1) = j$ avec $j \neq 1$, ce qui donne $n-1$ choix pour j.

— Si $\sigma(j) = 1$: les éléments restants forment un dérangement de $\{2, \ldots, n\} \setminus \{j\}$, d'où D_{n-2} possibilités.

— Si $\sigma(j) \neq 1$: on effectue la substitution $\sigma'(i) = \sigma(i)$ pour $i \neq 1$ et $\sigma'(j) = \sigma(j)$ sauf que l'interdiction $\sigma(j) \neq 1$ remplace $\sigma(j) \neq j$, donnant D_{n-1} possibilités.

D'où $D_n = (n-1)(D_{n-1} + D_{n-2})$. □

5.2.4 Le problème des ménages (aperçu)

Remarque 5.16 (Problème des ménages). Le *problème des ménages* demande de compter le nombre de façons d'asseoir n couples autour d'une table ronde de sorte qu'aucun époux ne soit à côté de son conjoint et que les places alternent hommes et femmes. La réponse, notée M_n, est donnée par la formule de Touchard :

$$M_n = n! \sum_{k=0}^{n} (-1)^k \frac{2n}{2n-k} \binom{2n-k}{k} (n-k)!$$

pour $n \geqslant 3$. La démonstration, qui repose sur une application raffinée de l'inclusion-exclusion, dépasse le cadre de ce cours.

5.3 Nombres de Stirling de seconde espèce

Définition 5.17 (Nombre de Stirling de seconde espèce)**.** Le *nombre de Stirling de seconde espèce* $\left\{ n \atop k \right\}$ est le nombre de partitions d'un ensemble à n éléments en exactement k blocs non vides. On le note aussi $S(n,k)$.

Théorème 5.18 (Récurrence de Stirling)**.** *Pour $n \geqslant 1$ et $1 \leqslant k \leqslant n$,*

$$\left\{ n \atop k \right\} = k \left\{ n-1 \atop k \right\} + \left\{ n-1 \atop k-1 \right\},$$

avec les conditions initiales $\left\{ 0 \atop 0 \right\} = 1$ et $\left\{ n \atop 0 \right\} = 0$ pour $n \geqslant 1$.

Démonstration. Considérons l'élément n dans une partition de $\{1, \ldots, n\}$ en k blocs.

— Si $\{n\}$ est un bloc à lui seul : les $n-1$ éléments restants forment une partition en $k-1$ blocs, d'où $\left\{ n-1 \atop k-1 \right\}$ possibilités.

— Si n est dans un bloc contenant d'autres éléments : on partitionne d'abord $\{1, \ldots, n-1\}$ en k blocs ($\left\{ n-1 \atop k \right\}$ façons), puis on insère n dans l'un des k blocs. □

Théorème 5.19 (Formule explicite de Stirling)**.** *Pour $n \geqslant k \geqslant 1$,*

$$\left\{ n \atop k \right\} = \frac{1}{k!} \sum_{j=0}^{k} (-1)^j \binom{k}{j} (k-j)^n.$$

Démonstration. Le nombre de surjections de $\{1, \ldots, n\}$ vers $\{1, \ldots, k\}$ est, d'une part, donné par le théorème 5.7 : $\sum_{j=0}^{k} (-1)^j \binom{k}{j} (k-j)^n$. D'autre part, chaque partition en k

$n\backslash k$	0	1	2	3	4	5	6
0	1	0	0	0	0	0	0
1	0	1	0	0	0	0	0
2	0	1	1	0	0	0	0
3	0	1	3	1	0	0	0
4	0	1	7	6	1	0	0
5	0	1	15	25	10	1	0
6	0	1	31	90	65	15	1

FIGURE 5.3 – Triangle des nombres de Stirling de seconde espèce $\left\{ {n \atop k} \right\}$ pour $0 \leqslant n \leqslant 6$.

blocs donne lieu à $k!$ surjections (en étiquetant les blocs). Donc le nombre de surjections est $k!\left\{ {n \atop k} \right\}$, ce qui donne la formule. □

Exemple 5.20. Calculons $\left\{ {4 \atop 2} \right\}$:

$$\left\{ {4 \atop 2} \right\} = \frac{1}{2!}\Big[\binom{2}{0}2^4 - \binom{2}{1}1^4 + \binom{2}{2}0^4\Big] = \frac{1}{2}(16 - 2 + 0) = 7.$$

Les 7 partitions de $\{1,2,3,4\}$ en 2 blocs sont : $\{\{1\},\{2,3,4\}\}$, $\{\{2\},\{1,3,4\}\}$, $\{\{3\},\{1,2,4\}\}$, $\{\{4\},\{1,2,3\}\}$, $\{\{1,2\},\{3,4\}\}$, $\{\{1,3\},\{2,4\}\}$, $\{\{1,4\},\{2,3\}\}$.

5.4 Nombres de Bell

Définition 5.21 (Nombre de Bell)**.** Le *nombre de Bell* B_n est le nombre total de partitions d'un ensemble à n éléments :

$$B_n = \sum_{k=0}^{n} \left\{ {n \atop k} \right\}.$$

Proposition 5.22 (Récurrence de Bell)**.** *Pour $n \geqslant 1$,*

$$B_n = \sum_{k=0}^{n-1} \binom{n-1}{k} B_k.$$

Démonstration. Le bloc contenant l'élément n contient $n-1-k$ autres éléments (choisis parmi les $n-1$ restants de $\binom{n-1}{n-1-k} = \binom{n-1}{k}$ façons), et les k éléments restants forment une partition arbitraire (B_k possibilités). En sommant sur $k = 0, \ldots, n-1$, on obtient la récurrence. □

Exemple 5.23 (Premières valeurs)**.**

$$B_0 = 1, \quad B_1 = 1, \quad B_2 = 2, \quad B_3 = 5, \quad B_4 = 15, \quad B_5 = 52, \quad B_6 = 203.$$

Remarque 5.24 (Formule de Dobinski). Les nombres de Bell admettent la représentation en série :

$$B_n = \frac{1}{e}\sum_{k=0}^{\infty}\frac{k^n}{k!}.$$

Cette formule, due à Dobinski (1877), sera retrouvée via les séries génératrices exponentielles au chapitre 6.

5.5 Partitions d'entiers (introduction)

Définition 5.25 (Partition d'un entier)**.** Une *partition* d'un entier positif n est une écriture $n = \lambda_1 + \lambda_2 + \cdots + \lambda_r$ avec $\lambda_1 \geqslant \lambda_2 \geqslant \cdots \geqslant \lambda_r \geqslant 1$. On note $p(n)$ le nombre de partitions de n.

Exemple 5.26. Les partitions de 5 sont : 5, $4+1$, $3+2$, $3+1+1$, $2+2+1$, $2+1+1+1$, $1+1+1+1+1$. Donc $p(5) = 7$.

Théorème 5.27 (Fonction génératrice des partitions)**.** *La série génératrice des $p(n)$ est*

$$\sum_{n=0}^{\infty} p(n)x^n = \prod_{k=1}^{\infty}\frac{1}{1-x^k}.$$

Idée de preuve. Chaque facteur $\frac{1}{1-x^k} = 1 + x^k + x^{2k} + \cdots$ encode le nombre de fois que la part k apparaît dans la partition. En multipliant sur tous les $k \geqslant 1$, on obtient exactement la somme sur toutes les partitions. □

Théorème 5.28 (Théorème d'Euler sur les partitions)**.** *Le nombre de partitions de n en parts impaires est égal au nombre de partitions de n en parts distinctes.*

Démonstration. Les partitions en parts distinctes ont pour génératrice $\prod_{k=1}^{\infty}(1+x^k)$. On a

$$\prod_{k=1}^{\infty}(1+x^k) = \prod_{k=1}^{\infty}\frac{1-x^{2k}}{1-x^k} = \frac{\prod_{k=1}^{\infty}(1-x^{2k})}{\prod_{k=1}^{\infty}(1-x^k)} = \prod_{\substack{k=1\\ k\text{ impair}}}^{\infty}\frac{1}{1-x^k},$$

qui est la génératrice des partitions en parts impaires. □

5.6 Exercices

Exercice 5.1 (Crible d'Ératosthène)**.** Utilisez le principe d'inclusion-exclusion pour déterminer le nombre de nombres premiers dans $\{1, 2, \ldots, 120\}$. *Indication* : il suffit de cribler par 2, 3, 5 et 7.

Exercice 5.2 (Fonctions à image prescrite)**.** Combien de fonctions $f : \{1, \ldots, 6\} \to \{a, b, c, d\}$ ont pour image exactement $\{a, b, c\}$?

Exercice 5.3 (Dérangements et probabilités)**.** Un professeur rend au hasard n copies à n étudiants. Quelle est la probabilité qu'aucun étudiant ne reçoive sa propre copie ? Calculer la limite quand $n \to \infty$.

Exercice 5.4 (Stirling et identités)**.** Montrez que pour tout $n \geqslant 1$:

$$\sum_{k=0}^{n} \left\{ n \atop k \right\} x^{\underline{k}} = x^n,$$

où $x^{\underline{k}} = x(x-1)\cdots(x-k+1)$ désigne la puissance descendante.

Exercice 5.5 (Surjections et nombres de Stirling)**.** En utilisant la relation entre surjections et nombres de Stirling, montrez que $\left\{ n \atop n-1 \right\} = \binom{n}{2}$ pour tout $n \geqslant 2$. Interprétez combinatoirement ce résultat.

Exercice 5.6 (Triangle de Bell)**.** Le *triangle de Bell* est construit comme suit : la première ligne contient $B_0 = 1$, et chaque ligne suivante commence par le dernier élément de la ligne précédente, les éléments suivants étant la somme de l'élément à gauche et de l'élément au-dessus. Construisez les 6 premières lignes et vérifiez que les premiers éléments de chaque ligne sont les nombres de Bell.

Exercice 5.7 (Indicatrice d'Euler)**.** a) Calculez $\varphi(1000)$ et $\varphi(2025)$.

b) Montrez que $\sum_{d \mid n} \varphi(d) = n$ en utilisant l'inclusion-exclusion.

Exercice 5.8 (Partitions en au plus k parts)**.** Montrez, par un argument de génératrices, que le nombre de partitions de n en au plus k parts est égal au nombre de partitions de n dont chaque part est $\leqslant k$.

Résumé du chapitre

- Le **principe d'inclusion-exclusion** donne $\operatorname{card} \bigcup A_i$ en termes des cardinaux des intersections, avec des signes alternés.
- Applications principales : **surjections** ($\sum (-1)^j \binom{k}{j} (k-j)^n$), **indicatrice d'Euler** ($\varphi(n) = n \prod (1 - 1/p_i)$), **dérangements** ($D_n = n! \sum (-1)^k / k!$).
- Les **nombres de Stirling de seconde espèce** $\left\{ n \atop k \right\}$ comptent les partitions d'ensembles en k blocs et sont liés aux surjections par $\left\{ n \atop k \right\} = S(n,k)/k!$.
- Les **nombres de Bell** $B_n = \sum_k \left\{ n \atop k \right\}$ comptent toutes les partitions d'un ensemble.
- Les **partitions d'entiers** $p(n)$ ont pour génératrice $\prod_k (1 - x^k)^{-1}$.

Chapitre 6

Séries Génératrices Ordinaires et Exponentielles

Les séries génératrices constituent l'un des outils les plus élégants et les plus puissants de la combinatoire. Elles transforment des problèmes de dénombrement en problèmes d'algèbre et d'analyse, permettant de résoudre des récurrences, d'obtenir des formules explicites et de démontrer des identités.

6.1 Séries génératrices ordinaires

Définition 6.1 (Série génératrice ordinaire)**.** Soit $(a_n)_{n\geqslant 0}$ une suite de nombres. La *série génératrice ordinaire* (SGO) de cette suite est la série formelle

$$A(x) = \sum_{n=0}^{\infty} a_n x^n.$$

Notation 6.2. On note $[x^n]A(x) = a_n$ le coefficient de x^n dans $A(x)$.

Exemple 6.3 (Exemples fondamentaux)**.**

i) La suite constante $a_n = 1$ a pour SGO $\dfrac{1}{1-x} = \displaystyle\sum_{n=0}^{\infty} x^n$.

ii) La suite $a_n = r^n$ a pour SGO $\dfrac{1}{1-rx} = \displaystyle\sum_{n=0}^{\infty} r^n x^n$.

iii) La suite $a_n = \binom{n+k-1}{k-1}$ a pour SGO $\dfrac{1}{(1-x)^k}$.

iv) La suite $a_n = \binom{m}{n}$ (avec m fixé) a pour SGO $(1+x)^m$.

6.1.1 Opérations sur les SGO

Proposition 6.4 (Addition et multiplication scalaire). *Si* $A(x) = \sum a_n x^n$ *et* $B(x) = \sum b_n x^n$, *alors*

$$\alpha A(x) + \beta B(x) = \sum_{n=0}^{\infty} (\alpha a_n + \beta b_n) x^n.$$

Théorème 6.5 (Produit de Cauchy (convolution)). *Si* $A(x) = \sum a_n x^n$ *et* $B(x) = \sum b_n x^n$, *alors*

$$A(x) \cdot B(x) = \sum_{n=0}^{\infty} c_n x^n, \quad \text{où} \quad c_n = \sum_{k=0}^{n} a_k b_{n-k}.$$

Démonstration. C'est la formule standard du produit de séries formelles, qui résulte de la distributivité : le terme $a_k x^k \cdot b_{n-k} x^{n-k} = a_k b_{n-k} x^n$ contribue au coefficient de x^n. □

Proposition 6.6 (Décalage). *Si* $A(x) = \sum_{n=0}^{\infty} a_n x^n$, *alors :*

i) $\dfrac{A(x) - a_0}{x} = \displaystyle\sum_{n=0}^{\infty} a_{n+1} x^n$ *(décalage à gauche).*

ii) $xA(x) = \sum_{n=1}^{\infty} a_{n-1} x^n$ *(décalage à droite).*

Proposition 6.7 (Dérivation). *Si* $A(x) = \sum_{n=0}^{\infty} a_n x^n$, *alors*

$$A'(x) = \sum_{n=0}^{\infty} (n+1) a_{n+1} x^n, \qquad xA'(x) = \sum_{n=0}^{\infty} n a_n x^n.$$

Plus généralement, l'opérateur $x\frac{d}{dx}$ *revient à multiplier* a_n *par* n.

Exemple 6.8 (Application de la dérivation). Calculons $\sum_{n=0}^{\infty} n x^n$. On part de $\frac{1}{1-x} = \sum x^n$ et on applique $x\frac{d}{dx}$:

$$x \cdot \frac{d}{dx} \frac{1}{1-x} = \frac{x}{(1-x)^2} = \sum_{n=0}^{\infty} n x^n.$$

En posant $x = 1/2$, on retrouve $\sum_{n=0}^{\infty} n/2^n = 2$.

6.1.2 Résolution de récurrences par SGO

Exemple 6.9 (Suite de Fibonacci via SGO). Résolvons la récurrence $F_0 = 0$, $F_1 = 1$, $F_n = F_{n-1} + F_{n-2}$ pour $n \geqslant 2$. Posons $F(x) = \sum_{n=0}^{\infty} F_n x^n$. La récurrence donne

$$F(x) - F_0 - F_1 x = x(F(x) - F_0) + x^2 F(x),$$

soit $F(x) - x = xF(x) + x^2F(x)$, d'où

$$F(x) = \frac{x}{1 - x - x^2}.$$

En décomposant en éléments simples avec les racines $\alpha = \frac{1+\sqrt{5}}{2}$ et $\beta = \frac{1-\sqrt{5}}{2}$ de $1 - x - x^2 = -(x - 1/\alpha)(x - 1/\beta)$, on obtient

$$F(x) = \frac{1}{\sqrt{5}}\left(\frac{1}{1-\alpha x} - \frac{1}{1-\beta x}\right),$$

ce qui donne la formule de Binet :

$$F_n = \frac{\alpha^n - \beta^n}{\sqrt{5}} = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right].$$

Exemple 6.10 (Récurrence linéaire d'ordre 2)**.** Résolvons $a_0 = 1$, $a_1 = 3$, $a_n = 4a_{n-1} - 4a_{n-2}$ pour $n \geqslant 2$. Posons $A(x) = \sum a_n x^n$. La récurrence donne

$$A(x) - 1 - 3x = 4x(A(x) - 1) - 4x^2A(x),$$

d'où $A(x)(1 - 4x + 4x^2) = 1 - x$, soit

$$A(x) = \frac{1 - x}{(1 - 2x)^2}.$$

En décomposant : $A(x) = \frac{1}{1-2x} + \frac{1}{(1-2x)^2}$ (après calcul). Or $[x^n]\frac{1}{(1-2x)^2} = (n + 1)2^n$, donc $a_n = 2^n + (n + 1)2^n = (n + 2)2^n$.

6.1.3 Les nombres de Catalan

Définition 6.11 (Nombre de Catalan)**.** Le n-ième *nombre de Catalan* est

$$C_n = \frac{1}{n+1}\binom{2n}{n}, \qquad n \geqslant 0.$$

Théorème 6.12 (SGO des nombres de Catalan)**.** *La série génératrice ordinaire* $C(x) = \sum_{n=0}^{\infty} C_n x^n$ *satisfait l'équation fonctionnelle*

$$C(x) = 1 + xC(x)^2,$$

et on a

$$C(x) = \frac{1 - \sqrt{1 - 4x}}{2x}.$$

Démonstration. Les nombres de Catalan satisfont la récurrence $C_0 = 1$ et $C_{n+1} = \sum_{k=0}^{n} C_k C_{n-k}$ pour $n \geqslant 0$ (décomposition récursive des chemins de Dyck, par exemple).

En termes de séries génératrices, cela se traduit par

$$\frac{C(x)-1}{x} = C(x)^2, \quad \text{soit} \quad C(x) = 1 + xC(x)^2.$$

C'est une équation du second degré en $C(x)$: $xC(x)^2 - C(x) + 1 = 0$, de discriminant $\Delta = 1 - 4x$, d'où

$$C(x) = \frac{1 \pm \sqrt{1-4x}}{2x}.$$

Comme $C(0) = 1$, on choisit le signe $-$ (le signe $+$ donnerait $C(x) \to \infty$ quand $x \to 0$).

Vérifions la formule du coefficient. En utilisant le binôme généralisé,

$$\sqrt{1-4x} = \sum_{n=0}^{\infty} \binom{1/2}{n} (-4x)^n,$$

on obtient, après simplification,

$$[x^n]C(x) = \frac{1}{n+1}\binom{2n}{n} = C_n. \qquad \square$$

Exemple 6.13 (Premières valeurs de Catalan)**.**

$$C_0 = 1,\ C_1 = 1,\ C_2 = 2,\ C_3 = 5,\ C_4 = 14,\ C_5 = 42,\ C_6 = 132,\ C_7 = 429.$$

Proposition 6.14 (Interprétations combinatoires de C_n)**.** *Le nombre C_n compte, entre autres :*

i) le nombre de chemins de Dyck de longueur $2n$ (chemins de $(0,0)$ à $(2n,0)$ avec des pas $+1$ et -1, ne passant jamais sous l'axe des abscisses) ;

ii) le nombre de parenthésages corrects de n paires de parenthèses ;

iii) le nombre d'arbres binaires complets à n nœuds internes ;

iv) le nombre de triangulations d'un polygone convexe à $n+2$ côtés.

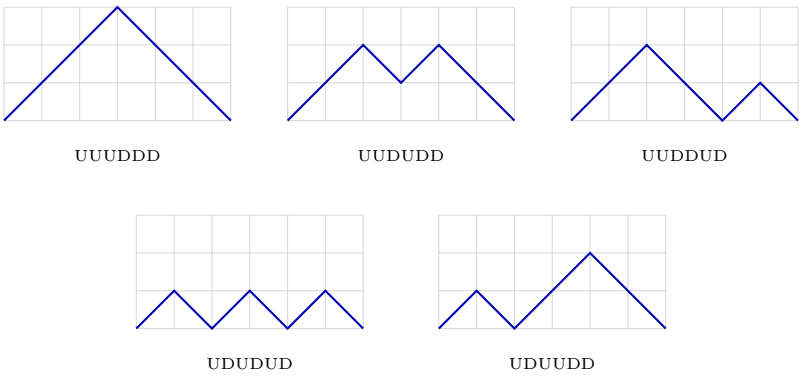


FIGURE 6.1 – Les $C_3 = 5$ chemins de Dyck de longueur 6. U = montée, D = descente.

6.2 Séries génératrices exponentielles

6.2.1 Définition et motivation

((())) (()()) (())() ()(()) ()()()

FIGURE 6.2 – Les $C_3 = 5$ parenthésages corrects de 3 paires de parenthèses.

Définition 6.15 (Série génératrice exponentielle)**.** Soit $(a_n)_{n\geqslant 0}$ une suite. La *série génératrice exponentielle* (SGE) de cette suite est

$$\hat{A}(x) = \sum_{n=0}^{\infty} a_n \frac{x^n}{n!}.$$

Remarque 6.16. La SGE est particulièrement adaptée au dénombrement de structures *étiquetées* (permutations, graphes étiquetés, etc.), car le facteur $1/n!$ dans la série compense le nombre de réétiquetages.

Exemple 6.17 (SGE fondamentales)**.** i) La suite $a_n = 1$ a pour SGE $e^x = \sum \frac{x^n}{n!}$.
ii) La suite $a_n = n!$ (nombre de permutations) a pour SGE $\frac{1}{1-x} = \sum x^n$.
iii) La suite $a_n = r^n$ a pour SGE e^{rx}.

Théorème 6.18 (Produit de SGE et structures étiquetées)**.** *Si* $\hat{A}(x) = \sum a_n \frac{x^n}{n!}$ *et* $\hat{B}(x) = \sum b_n \frac{x^n}{n!}$*, alors*

$$\hat{A}(x) \cdot \hat{B}(x) = \sum_{n=0}^{\infty} c_n \frac{x^n}{n!}, \quad \text{où} \quad c_n = \sum_{k=0}^{n} \binom{n}{k} a_k b_{n-k}.$$

Démonstration. On a

$$\hat{A}(x) \cdot \hat{B}(x) = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} \frac{a_k}{k!} \cdot \frac{b_{n-k}}{(n-k)!} \right) x^n = \sum_{n=0}^{\infty} \frac{1}{n!} \left(\sum_{k=0}^{n} \binom{n}{k} a_k b_{n-k} \right) \frac{x^n}{1}.$$

En identifiant, on obtient $c_n = \sum_k \binom{n}{k} a_k b_{n-k}$, qui est la *convolution binomiale*. □

Remarque 6.19 (Interprétation combinatoire). Si a_n compte les structures de type $\mathcal{A}$ sur n éléments et b_n celles de type $\mathcal{B}$, alors c_n compte les structures obtenues en partitionnant $\{1, \ldots, n\}$ en deux parts, plaçant une $\mathcal{A}$-structure sur la première et une $\mathcal{B}$-structure sur la seconde. C'est le *produit étiqueté* de la combinatoire analytique.

6.2.2 SGE des permutations

Exemple 6.20 (Permutations et SGE)**.** Puisque le nombre de permutations de

$\{1, \ldots, n\}$ est $n!$, la SGE des permutations est

$$\sum_{n=0}^{\infty} n! \cdot \frac{x^n}{n!} = \sum_{n=0}^{\infty} x^n = \frac{1}{1-x}.$$

Exemple 6.21 (Involutions)**.** Une *involution* est une permutation σ telle que $\sigma^2 = \mathrm{id}$. Si I_n désigne le nombre d'involutions de $\{1, \ldots, n\}$, on a la récurrence $I_n = I_{n-1} + (n-1)I_{n-2}$ (l'élément n est soit un point fixe, soit échangé avec l'un des $n-1$ autres éléments). La SGE satisfait

$$\hat{I}'(x) = (1+x)\hat{I}(x), \qquad \hat{I}(0) = 1,$$

d'où $\hat{I}(x) = e^{x+x^2/2}$.

6.2.3 SGE des dérangements

Théorème 6.22 (SGE des dérangements)**.** *La SGE des dérangements est*

$$\hat{D}(x) = \sum_{n=0}^{\infty} D_n \frac{x^n}{n!} = \frac{e^{-x}}{1-x}.$$

Démonstration. Toute permutation se décompose de manière unique en un ensemble de points fixes et un dérangement du reste. Si $\hat{D}(x)$ est la SGE des dérangements, la SGE des permutations (qui est $1/(1-x)$) s'écrit comme le produit de la SGE de l'identité sur les points fixes (e^x, car un ensemble de k points fixes se choisit de $\binom{n}{k}$ manières) et de $\hat{D}(x)$:

$$\frac{1}{1-x} = e^x \cdot \hat{D}(x),$$

d'où $\hat{D}(x) = \frac{e^{-x}}{1-x}$.

Vérifions : en développant,

$$\hat{D}(x) = \left(\sum_{k=0}^{\infty} \frac{(-x)^k}{k!}\right)\left(\sum_{m=0}^{\infty} x^m\right) = \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n} \frac{(-1)^k}{k!}\right) x^n.$$

Le coefficient de x^n est $\sum_{k=0}^{n} \frac{(-1)^k}{k!} = D_n/n!$, ce qui correspond bien à la formule du théorème 5.13. □

6.2.4 SGE des nombres de Bell

Théorème 6.23 (SGE des nombres de Bell)**.** *La SGE des nombres de Bell est*

$$\sum_{n=0}^{\infty} B_n \frac{x^n}{n!} = e^{e^x - 1}.$$

Démonstration. Une partition d'un ensemble étiqueté peut être vue comme un ensemble (non ordonné) de blocs non vides. En combinatoire analytique, la SGE d'un ensemble de structures ayant pour SGE $\hat{B}(x)$ est $e^{\hat{B}(x)}$. La SGE d'un bloc non vide (ensemble non vide) est $e^x - 1$. Donc la SGE des partitions est e^{e^x-1}.

Plus directement, on vérifie que la récurrence $B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k$ (proposition 5.22) est compatible avec cette SGE en dérivant :

$$\frac{d}{dx} e^{e^x-1} = e^x \cdot e^{e^x-1},$$

ce qui signifie $B_{n+1}/n! = \sum_{k=0}^{n} B_k/(k! \cdot (n-k)!)$, soit $B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k$. □

Corollaire 6.24 (Formule de Dobinski)**.** *Pour tout $n \geqslant 0$,*

$$B_n = \frac{1}{e} \sum_{k=0}^{\infty} \frac{k^n}{k!}.$$

Démonstration. On développe $e^{e^x-1} = e^{-1}e^{e^x} = e^{-1} \sum_{k=0}^{\infty} \frac{e^{kx}}{k!} = e^{-1} \sum_{k=0}^{\infty} \frac{1}{k!} \sum_{n=0}^{\infty} \frac{(kx)^n}{n!}$. En échangeant les sommations et en identifiant le coefficient de $x^n/n!$: $B_n = e^{-1} \sum_{k=0}^{\infty} k^n/k!$. □

6.3 Séries formelles : structure d'anneau

Définition 6.25 (Anneau des séries formelles)**.** L'ensemble $\mathbb{R}[[x]]$ des séries formelles à coefficients réels, muni de l'addition et de la multiplication (produit de Cauchy), forme un anneau commutatif unitaire. Plus précisément, si $A(x) = \sum a_n x^n$ et $B(x) = \sum b_n x^n$, alors :

- $(A + B)(x) = \sum (a_n + b_n) x^n$,
- $(A \cdot B)(x) = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_k b_{n-k} \right) x^n$.

L'élément neutre pour l'addition est 0 et pour la multiplication est 1.

Proposition 6.26 (Inversibilité)**.** *Une série formelle $A(x) = \sum_{n=0}^{\infty} a_n x^n$ est inversible dans $\mathbb{R}[[x]]$ si et seulement si $a_0 \neq 0$.*

Démonstration. Si $A(x)B(x) = 1$, en identifiant le terme constant on obtient $a_0 b_0 = 1$, donc $a_0 \neq 0$ est nécessaire. Réciproquement, si $a_0 \neq 0$, on peut construire les coefficients b_n de $B(x)$ par récurrence : $b_0 = 1/a_0$ et pour $n \geqslant 1$,

$$b_n = -\frac{1}{a_0} \sum_{k=1}^{n} a_k b_{n-k}.$$

□

Proposition 6.27 (Composition)**.** *Si $A(x) = \sum a_n x^n$ et $B(x) = \sum_{n=1}^{\infty} b_n x^n$ (avec $b_0 = 0$), alors la série composée $A(B(x))$ est bien définie dans $\mathbb{R}[[x]]$.*

Remarque 6.28. L'anneau $\mathbb{R}[[x]]$ est intègre (produit de séries non nulles est non nul) mais pas un corps. Cependant, le corps des fractions de $\mathbb{R}[[x]]$ est l'ensemble $\mathbb{R}((x))$ des *séries de Laurent formelles*.

6.4 Exemples développés

6.4.1 Fibonacci via SGO : méthode complète

Exemple 6.29 (Fibonacci : résolution détaillée)**.** Reprenons $F(x) = x/(1-x-x^2)$. Les racines de $1 - x - x^2 = 0$ sont $x = (-1 \pm \sqrt{5})/2$, donc $1/\alpha$ et $1/\beta$ où $\alpha = (1+\sqrt{5})/2$ (nombre d'or) et $\beta = (1-\sqrt{5})/2$. Ainsi $1 - x - x^2 = -(x - 1/\alpha)(x - 1/\beta) = (1-\alpha x)(1-\beta x)/(\alpha\beta)$. Comme $\alpha\beta = -1$, on a $1-x-x^2 = -(1-\alpha x)(1-\beta x)\cdot(-1) = (1-\alpha x)(1-\beta x)$.
Vérifions : $(1-\alpha x)(1-\beta x) = 1 - (\alpha+\beta)x + \alpha\beta x^2 = 1 - x - x^2$. ✓
Décomposition en éléments simples :

$$F(x) = \frac{x}{(1-\alpha x)(1-\beta x)} = \frac{A}{1-\alpha x} + \frac{B}{1-\beta x}.$$

En posant $x = 1/\alpha$: $A = \frac{1/\alpha}{1-\beta/\alpha} = \frac{1}{\alpha-\beta} = \frac{1}{\sqrt{5}}$. De même, $B = -1/\sqrt{5}$. Donc

$$F_n = \frac{\alpha^n - \beta^n}{\sqrt{5}}.$$

Puisque $|\beta| < 1$, on a $F_n = \lfloor \alpha^n/\sqrt{5} + 1/2 \rfloor$ pour tout $n \geqslant 0$.

6.4.2 Dérangements via SGE : vérification

Exemple 6.30 (Dérangements : extraction de coefficients)**.** À partir de $\hat{D}(x) = e^{-x}/(1-x)$, extrayons D_n directement. On a

$$\hat{D}(x) = \left(\sum_{j=0}^{\infty} \frac{(-1)^j x^j}{j!}\right)\left(\sum_{m=0}^{\infty} x^m\right).$$

Le coefficient de x^n est

$$\sum_{j=0}^{n} \frac{(-1)^j}{j!} \cdot 1 = \sum_{j=0}^{n} \frac{(-1)^j}{j!} = \frac{D_n}{n!},$$

d'où $D_n = n! \sum_{j=0}^{n} (-1)^j/j!$, conformément au théorème 5.13.

Vérification numérique. Pour $n = 4$: $D_4 = 24(1-1+1/2-1/6+1/24) = 24\cdot 3/8 = 9$. Effectivement, les 9 dérangements de $\{1,2,3,4\}$ sont : $(2,1,4,3)$, $(2,3,4,1)$, $(2,4,1,3)$, $(3,1,4,2)$, $(3,4,1,2)$, $(3,4,2,1)$, $(4,1,2,3)$, $(4,3,1,2)$, $(4,3,2,1)$.

6.4.3 Nombres de Catalan : récurrence et formule close

Exemple 6.31 (Catalan via l'équation fonctionnelle)**.** De l'équation $C(x) = 1+xC(x)^2$, on peut extraire la récurrence directement. Le coefficient de x^{n+1} dans $xC(x)^2$ est $[x^n]C(x)^2 = \sum_{k=0}^{n} C_k C_{n-k}$, d'où

$$C_{n+1} = \sum_{k=0}^{n} C_k C_{n-k}.$$

Calculons : $C_0 = 1$, $C_1 = C_0^2 = 1$, $C_2 = C_0C_1 + C_1C_0 = 2$, $C_3 = C_0C_2 + C_1^2 + C_2C_0 = 2 + 1 + 2 = 5$, $C_4 = 2 \cdot 5 + 2 \cdot 2 + 5 \cdot 1 = 14$.

6.4.4 Application : chemins dans un réseau

Exemple 6.32 (Chemins de réseau)**.** Le nombre de chemins du point $(0, 0)$ au point (m, n) dans $\mathbb{Z}^2$, n'utilisant que des pas vers la droite $(1, 0)$ ou vers le haut $(0, 1)$, est $\binom{m+n}{m}$. La SGO en deux variables est

$$\sum_{m,n\geqslant 0} \binom{m+n}{m} x^m y^n = \frac{1}{1-x-y}.$$

C'est un cas particulier du produit de SGO : le chemin est une suite de $m + n$ pas, dont m sont horizontaux.

6.5 Techniques avancées

Proposition 6.33 (Extraction via le binôme généralisé)**.** *Pour tout $\alpha \in \mathbb{R}$ et $|x| < 1$,*

$$(1+x)^\alpha = \sum_{n=0}^{\infty} \binom{\alpha}{n} x^n, \quad \text{où} \quad \binom{\alpha}{n} = \frac{\alpha(\alpha-1)\cdots(\alpha-n+1)}{n!}.$$

Exemple 6.34 (Coefficients centraux)**.** De $(1-4x)^{-1/2} = \sum_{n=0}^{\infty} \binom{2n}{n} x^n$, on déduit que

$$\binom{-1/2}{n}(-4)^n = \frac{(-1/2)(-3/2)\cdots(-(2n-1)/2)}{n!}(-4)^n = \binom{2n}{n}.$$

Proposition 6.35 (Méthode du serpent (snake oil))**.** *Pour évaluer une somme $S = \sum_k f(n, k)$ faisant intervenir des coefficients binomiaux, on forme la SGO $F(x) = \sum_n S_n x^n$, on intervertit les sommations, et on simplifie le résultat à l'aide de séries connues.*

Exemple 6.36 (Identité de Vandermonde via SGO)**.** Montrons que $\sum_{k=0}^{r} \binom{m}{k}\binom{n}{r-k} = \binom{m+n}{r}$. On compare les coefficients de x^r dans $(1+x)^m(1+x)^n = (1+x)^{m+n}$. Le membre gauche donne $\sum_k \binom{m}{k}\binom{n}{r-k}$ (produit de Cauchy) et le membre droit donne $\binom{m+n}{r}$.

6.6 Exercices

Exercice 6.1 (SGO et coefficients binomiaux)**.** Montrez que la SGO de la suite $a_n = \binom{2n}{n}$ est $\frac{1}{\sqrt{1-4x}}$.

Exercice 6.2 (Récurrence de Catalan)**.** Démontrez que $C_n = \frac{4n-2}{n+1}C_{n-1}$ pour $n \geqslant 1$ à partir de la formule $C_n = \binom{2n}{n}/(n+1)$.

Exercice 6.3 (Suite de tribonacci)**.** La suite de tribonacci est définie par $T_0 = 0$, $T_1 = 0$, $T_2 = 1$ et $T_n = T_{n-1} + T_{n-2} + T_{n-3}$ pour $n \geqslant 3$. Déterminez sa SGO.

Exercice 6.4 (Nombre de façons de rendre la monnaie)**.** Avec des pièces de 1, 2 et 5 centimes, de combien de façons peut-on constituer une somme de n centimes ? Exprimez la réponse comme coefficient d'une SGO et calculez le résultat pour $n = 10$.

Exercice 6.5 (SGE et permutations sans point fixe)**.** En utilisant la SGE des dérangements, montrez que la probabilité qu'une permutation aléatoire de $\{1, \ldots, n\}$ soit un dérangement tend vers $1/e$ quand $n \to \infty$.

Exercice 6.6 (Nombres de Bell et congruence)**.** Montrez que $B_{p+1} \equiv B_1 + B_0 \pmod{p}$ pour tout nombre premier p, c'est-à-dire $B_{p+1} \equiv 2 \pmod{p}$ (théorème de Touchard). *Indication* : utiliser la formule de Dobinski modulo p.

Exercice 6.7 (Produit de SGE)**.** Soient $a_n = 2^n$ et $b_n = n!$. Calculez la suite $c_n = \sum_{k=0}^{n} \binom{n}{k} a_k b_{n-k}$ à l'aide du produit des SGE et donnez les cinq premières valeurs.

Exercice 6.8 (Arbres binaires et Catalan)**.** Soit T_n le nombre d'arbres binaires à n nœuds internes.

a) Montrez que $T_n = C_n$ en établissant que la SGO $T(x)$ satisfait $T(x) = 1 + xT(x)^2$.

b) Déduisez-en que le nombre d'arbres binaires à 10 nœuds internes est $C_{10} = 16\,796$.

Exercice 6.9 (Identité de Cauchy)**.** En utilisant les SGE, montrez l'identité

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

Indication : considérer $[x^n](1+x)^n(1+x)^n$.

Exercice 6.10 (Série génératrice des partitions en parts distinctes)**.** Montrez que la SGO des partitions de n en parts distinctes est $\prod_{k=1}^{\infty}(1+x^k)$ et calculez le nombre de telles partitions pour $n = 8$.

Résumé du chapitre

— La **série génératrice ordinaire** (SGO) $A(x) = \sum a_n x^n$ encode une suite (a_n). Le produit de SGO correspond à la **convolution** $c_n = \sum_k a_k b_{n-k}$.
— Les SGO permettent de résoudre des **récurrences linéaires** en les transformant en équations algébriques, puis en extrayant les coefficients par décomposition en éléments simples.
— Les **nombres de Catalan** $C_n = \binom{2n}{n}/(n+1)$ ont pour SGO $C(x) = (1 - \sqrt{1-4x})/(2x)$, satisfaisant $C = 1 + xC^2$.
— La **série génératrice exponentielle** (SGE) $\hat{A}(x) = \sum a_n x^n/n!$ est adaptée aux structures étiquetées. Le produit de SGE correspond à la **convolution binomiale**.
— SGE remarquables : permutations $\to 1/(1-x)$, dérangements $\to e^{-x}/(1-x)$, nombres de Bell $\to e^{e^x-1}$.
— L'anneau $\mathbb{R}[[x]]$ des séries formelles est commutatif, unitaire, intègre, et une série y est inversible ssi son terme constant est non nul.

Chapitre 7

Récurrences et Équations de Récurrence

Contents

Introduction

Les suites définies par récurrence sont omniprésentes en mathématiques discrètes et en informatique. Qu'il s'agisse de compter des configurations combinatoires, d'analyser la complexité d'un algorithme ou de modéliser un phénomène discret, on est souvent amené à exprimer le n-ième terme d'une suite en fonction des termes précédents. L'objectif de ce chapitre est de développer les techniques permettant de résoudre de telles *équations de récurrence*, c'est-à-dire de trouver une formule explicite (dite *forme close*) pour le terme général.

7.1 Récurrences linéaires à coefficients constants

7.1.1 Définitions et cadre général

Définition 7.1 (Récurrence linéaire d'ordre k)**.** Une **récurrence linéaire d'ordre k à coefficients constants** est une relation de la forme

$$a_n = c_1\, a_{n-1} + c_2\, a_{n-2} + \cdots + c_k\, a_{n-k} + f(n), \qquad n \geq k,$$

où $c_1, c_2, \ldots, c_k \in \mathbb{R}$ avec $c_k \neq 0$, et $f\colon \mathbb{N} \to \mathbb{R}$. La récurrence est dite **homogène** si $f(n) = 0$ pour tout n, et **non homogène** sinon.

Remarque 7.2. Pour qu'une telle récurrence détermine une suite unique, il faut spécifier k conditions initiales : $a_0, a_1, \ldots, a_{k-1}$.

7.1.2 Récurrences homogènes : l'équation caractéristique

Considérons la récurrence homogène d'ordre k :

$$a_n - c_1\, a_{n-1} - c_2\, a_{n-2} - \cdots - c_k\, a_{n-k} = 0. \tag{7.1}$$

Définition 7.3 (Équation caractéristique)**.** L'**équation caractéristique** associée à (7.1) est le polynôme

$$r^k - c_1\, r^{k-1} - c_2\, r^{k-2} - \cdots - c_k = 0. \tag{7.2}$$

L'idée fondatrice est de chercher des solutions de la forme $a_n = r^n$ pour une constante $r \neq 0$. En substituant dans (7.1), on obtient

$$r^n - c_1\, r^{n-1} - c_2\, r^{n-2} - \cdots - c_k\, r^{n-k} = 0.$$

En divisant par $r^{n-k} \neq 0$, on retrouve exactement (7.2).

Théorème 7.4 (Cas des racines distinctes)**.** *Si l'équation caractéristique (7.2) admet k racines distinctes $r_1, r_2, \ldots, r_k$ (dans $\mathbb{C}$), alors la solution générale de (7.1) est*

$$a_n = \alpha_1\, r_1^n + \alpha_2\, r_2^n + \cdots + \alpha_k\, r_k^n,$$

où les constantes $\alpha_1, \ldots, \alpha_k$ sont déterminées par les conditions initiales.

Démonstration. Montrons d'abord que l'ensemble $\mathcal{S}$ des suites satisfaisant (7.1) est un espace vectoriel (sur $\mathbb{R}$ ou $\mathbb{C}$) de dimension k.

Sous-espace vectoriel. Si (a_n) et (b_n) satisfont (7.1), alors pour tous $\lambda, \mu \in \mathbb{R}$, la suite $(\lambda a_n + \mu b_n)$ satisfait aussi (7.1) par linéarité.

Dimension k. L'application $\varphi\colon \mathcal{S} \to \mathbb{R}^k$ définie par $\varphi\big((a_n)\big) = (a_0, a_1, \ldots, a_{k-1})$ est un isomorphisme d'espaces vectoriels : elle est linéaire, injective (les conditions initiales déterminent la suite de manière unique) et surjective (pour tout choix de conditions initiales, il existe une unique suite solution).

Or les k suites $(r_i^n)_{n\geq 0}$ pour $i = 1, \dots, k$ sont solutions (par construction de l'équation caractéristique). Elles sont linéairement indépendantes car la matrice de Vandermonde

$$V = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ r_1 & r_2 & \cdots & r_k \\ r_1^2 & r_2^2 & \cdots & r_k^2 \\ \vdots & \vdots & \ddots & \vdots \\ r_1^{k-1} & r_2^{k-1} & \cdots & r_k^{k-1} \end{pmatrix}$$

a pour déterminant $\det(V) = \prod_{1\leq i<j\leq k}(r_j - r_i) \neq 0$ puisque les racines sont distinctes. Ainsi les (r_i^n) forment une base de $\mathcal{S}$. □

Théorème 7.5 (Cas des racines répétées)**.** *Si l'équation caractéristique (7.2) admet les racines $r_1, r_2, \dots, r_s$ de multiplicités respectives $m_1, m_2, \dots, m_s$ (avec $m_1 + m_2 + \cdots + m_s = k$), alors la solution générale est*

$$a_n = \sum_{i=1}^{s} \left(\alpha_{i,0} + \alpha_{i,1}\, n + \alpha_{i,2}\, n^2 + \cdots + \alpha_{i,m_i-1}\, n^{m_i-1}\right) r_i^n.$$

Démonstration. Il suffit de montrer que si r est une racine de multiplicité m du polynôme caractéristique $p(r)$, alors les suites $n^j r^n$ pour $j = 0, 1, \dots, m-1$ sont solutions de la récurrence.

Posons $a_n = n^j r^n$. L'opérateur de décalage E agit par $(Ea)_n = a_{n+1}$. La récurrence (7.1) se réécrit $p(E)\, a = 0$ où $p(x) = x^k - c_1 x^{k-1} - \cdots - c_k$. Puisque r est racine de multiplicité m, on a $p(x) = (x-r)^m\, q(x)$. Or l'opérateur $(E - r)$ appliqué à la suite $n^j r^n$ donne :

$$(E-r)(n^j r^n) = (n+1)^j r^{n+1} - r \cdot n^j r^n = r^{n+1}\big((n+1)^j - n^j\big),$$

qui est de la forme $r^{n+1}\cdot$(polynôme de degré $j-1$ en n). Par récurrence, $(E-r)^m(n^j r^n) = 0$ dès que $j < m$. Donc $p(E)(n^j r^n) = (E-r)^m q(E)(n^j r^n)$ et il suffit de vérifier que $(E-r)^m$ annule le résultat, ce qui découle de l'observation précédente appliquée au polynôme en n de degré au plus $j < m$.

L'indépendance linéaire des k solutions ainsi obtenues se vérifie par un argument de type Vandermonde généralisé (matrice confluente de Vandermonde). □

Exemple 7.6 (Récurrence d'ordre 2 à racines distinctes)**.** Résolvons $a_n = 5a_{n-1} - 6a_{n-2}$ avec $a_0 = 1$, $a_1 = 4$.
L'équation caractéristique est $r^2 - 5r + 6 = 0$, soit $(r-2)(r-3) = 0$. Les racines sont $r_1 = 2$ et $r_2 = 3$. La solution générale est $a_n = \alpha\, 2^n + \beta\, 3^n$.
Conditions initiales :

$$\begin{cases} \alpha + \beta = 1, \\ 2\alpha + 3\beta = 4. \end{cases} \quad \Longrightarrow \quad \alpha = -1, \quad \beta = 2.$$

Donc $a_n = -2^n + 2 \cdot 3^n = 2 \cdot 3^n - 2^n$.

Exemple 7.7 (Récurrence à racine double)**.** Résolvons $a_n = 4a_{n-1} - 4a_{n-2}$ avec $a_0 = 1$, $a_1 = 6$.
L'équation caractéristique est $r^2 - 4r + 4 = 0$, soit $(r-2)^2 = 0$. La racine double est $r = 2$. La solution générale est $a_n = (\alpha + \beta\, n)\, 2^n$.
Conditions initiales :

$$\begin{cases} \alpha = 1, \\ (\alpha + \beta) \cdot 2 = 6. \end{cases} \quad \Longrightarrow \quad \alpha = 1, \quad \beta = 2.$$

Donc $a_n = (1 + 2n)\, 2^n$.

Exemple 7.8 (Récurrence d'ordre 3)**.** Résolvons $a_n = 6a_{n-1} - 11a_{n-2} + 6a_{n-3}$ avec $a_0 = 2$, $a_1 = 5$, $a_2 = 15$.
L'équation caractéristique est $r^3 - 6r^2 + 11r - 6 = 0$, qui se factorise en $(r-1)(r-2)(r-3) = 0$. La solution générale est $a_n = \alpha + \beta\, 2^n + \gamma\, 3^n$.
Le système des conditions initiales donne $\alpha = 1$, $\beta = -1$, $\gamma = 2$, d'où $a_n = 1 - 2^n + 2 \cdot 3^n$.

7.1.3 Récurrences non homogènes

Théorème 7.9 (Structure des solutions d'une récurrence non homogène)**.** *La solution générale de la récurrence non homogène*

$$a_n - c_1 a_{n-1} - \cdots - c_k a_{n-k} = f(n)$$

est de la forme $a_n = a_n^{(h)} + a_n^{(p)}$, où $a_n^{(h)}$ est la solution générale de la récurrence homogène associée et $a_n^{(p)}$ est une solution particulière quelconque de la récurrence non homogène.

Démonstration. Si (a_n) et (b_n) sont deux solutions de la récurrence non homogène, alors leur différence $(a_n - b_n)$ satisfait la récurrence homogène, car

$$(a_n - b_n) - c_1(a_{n-1} - b_{n-1}) - \cdots - c_k(a_{n-k} - b_{n-k}) = f(n) - f(n) = 0. \qquad \square$$

Méthode des coefficients indéterminés

La forme de la solution particulière dépend de la forme du second membre $f(n)$.

Forme de $f(n)$	**Essai pour $a_n^{(p)}$**
d (constante)	A
$dn + e$	$An + B$
Polynôme de degré s	Polynôme de degré s
$d\,\beta^n$	$A\,\beta^n$
$n^s\,\beta^n$	$(A_0 + A_1 n + \cdots + A_s n^s)\,\beta^n$

Remarque 7.10. Si l'essai pour $a_n^{(p)}$ est lui-même solution de la récurrence homogène (c'est-à-dire si β est racine de l'équation caractéristique de multiplicité m), on multiplie l'essai par n^m.

Exemple 7.11 (Récurrence non homogène avec second membre constant)**.** Résolvons $a_n = 3a_{n-1} + 4$ avec $a_0 = 1$.
La récurrence homogène $a_n = 3a_{n-1}$ a pour solution $a_n^{(h)} = \alpha\, 3^n$. On cherche une solution particulière constante $a_n^{(p)} = A$. En substituant : $A = 3A + 4$, d'où $A = -2$.
Solution générale : $a_n = \alpha\, 3^n - 2$. Avec $a_0 = 1$: $\alpha - 2 = 1$, soit $\alpha = 3$. Conclusion : $a_n = 3^{n+1} - 2$.

Exemple 7.12 (Récurrence non homogène avec second membre polynomial)**.** Résolvons $a_n = 2a_{n-1} + n$ avec $a_0 = 0$.
Solution homogène : $a_n^{(h)} = \alpha\, 2^n$. On essaie $a_n^{(p)} = An + B$. En substituant :

$$An + B = 2(A(n-1) + B) + n = (2A + 1)n + (-2A + 2B).$$

Par identification : $A = 2A + 1$ et $B = -2A + 2B$, d'où $A = -1$, $B = -2$.
Solution générale : $a_n = \alpha\, 2^n - n - 2$. Avec $a_0 = 0$: $\alpha = 2$, d'où $a_n = 2^{n+1} - n - 2$.

Exemple 7.13 (Second membre exponentiel coïncidant avec la racine)**.** Résolvons $a_n = 2a_{n-1} + 2^n$ avec $a_0 = 1$.
La racine de l'équation caractéristique est $r = 2$, qui coïncide avec la base de l'exponentielle du second membre. On essaie donc $a_n^{(p)} = An \cdot 2^n$. En substituant :

$$An\, 2^n = 2 \cdot A(n-1)\, 2^{n-1} + 2^n = A(n-1)\, 2^n + 2^n.$$

Simplifiant par 2^n : $An = An - A + 1$, soit $A = 1$.
Solution générale : $a_n = \alpha\, 2^n + n\, 2^n = (\alpha + n)\, 2^n$. Avec $a_0 = 1$: $\alpha = 1$, d'où $a_n = (n+1)\, 2^n$.

7.2 La suite de Fibonacci et la formule de Binet

Définition 7.14 (Suite de Fibonacci)**.** La **suite de Fibonacci** $(F_n)_{n\geq 0}$ est définie par

$$F_0 = 0, \qquad F_1 = 1, \qquad F_n = F_{n-1} + F_{n-2} \quad (n \geq 2).$$

Les premiers termes sont : $0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \ldots$

Théorème 7.15 (Formule de Binet)**.** *Pour tout* $n \geq 0$,

$$F_n = \frac{\varphi^n - \psi^n}{\sqrt{5}},$$

où $\varphi = \dfrac{1+\sqrt{5}}{2}$ *(le* nombre d'or*) et* $\psi = \dfrac{1-\sqrt{5}}{2}$.

Démonstration. L'équation caractéristique de $F_n = F_{n-1} + F_{n-2}$ est $r^2 - r - 1 = 0$, de discriminant $\Delta = 5$. Les racines sont

$$\varphi = \frac{1+\sqrt{5}}{2} \approx 1{,}618 \quad \text{et} \quad \psi = \frac{1-\sqrt{5}}{2} \approx -0{,}618.$$

Elles sont distinctes, donc $F_n = \alpha\,\varphi^n + \beta\,\psi^n$. Les conditions initiales donnent le système :

$$\begin{cases} \alpha + \beta = F_0 = 0, \\ \alpha\,\varphi + \beta\,\psi = F_1 = 1. \end{cases}$$

De la première équation, $\beta = -\alpha$. En substituant dans la seconde : $\alpha(\varphi - \psi) = 1$, soit $\alpha\sqrt{5} = 1$, d'où $\alpha = 1/\sqrt{5}$ et $\beta = -1/\sqrt{5}$. □

Corollaire 7.16. *Pour tout* $n \geq 0$, F_n *est l'entier le plus proche de* $\varphi^n/\sqrt{5}$. *Plus précisément,* $\left|F_n - \varphi^n/\sqrt{5}\right| < 1/2$.

Démonstration. On a $|\psi| = \left|(1-\sqrt{5})/2\right| \approx 0{,}618 < 1$, donc $\left|\psi^n/\sqrt{5}\right| < 1/\sqrt{5} < 1/2$ pour tout $n \geq 0$. □

Proposition 7.17 (Identité de Cassini)**.** *Pour tout* $n \geq 1$,

$$F_{n-1}\,F_{n+1} - F_n^2 = (-1)^n.$$

Démonstration. Par récurrence sur n. Pour $n = 1$: $F_0 \cdot F_2 - F_1^2 = 0 \cdot 1 - 1 = -1 = (-1)^1$.

Supposons le résultat vrai au rang n. Alors

$$\begin{aligned} F_nF_{n+2} - F_{n+1}^2 &= F_n(F_{n+1} + F_n) - F_{n+1}^2 \\ &= F_nF_{n+1} + F_n^2 - F_{n+1}^2 \\ &= F_nF_{n+1} + F_n^2 - F_{n+1}(F_n + F_{n-1}) \\ &= F_n^2 - F_{n+1}F_{n-1} \\ &= -(F_{n-1}F_{n+1} - F_n^2) = -(-1)^n = (-1)^{n+1}. \end{aligned}$$

□

7.3 Exemples classiques de récurrences

7.3.1 Les tours de Hanoï

Définition 7.18 (Tours de Hanoï)**.** Soit T_n le nombre minimal de déplacements nécessaires pour transférer une tour de n disques d'un piquet à un autre, selon les règles classiques (un seul disque déplacé à la fois, jamais un grand disque sur un petit).

Proposition 7.19. *La suite (T_n) satisfait la récurrence $T_n = 2T_{n-1} + 1$ avec $T_1 = 1$, et a pour forme close $T_n = 2^n - 1$.*

Démonstration. Récurrence. Pour déplacer n disques du piquet A au piquet C :

(i) déplacer les $n-1$ disques supérieurs de A vers B (T_{n-1} coups) ;

(ii) déplacer le disque le plus grand de A vers C (1 coup) ;

(iii) déplacer les $n-1$ disques de B vers C (T_{n-1} coups).

Donc $T_n = 2T_{n-1} + 1$.

Forme close. Posons $S_n = T_n + 1$. Alors $S_n = 2S_{n-1}$ avec $S_1 = 2$, d'où $S_n = 2^n$ et $T_n = 2^n - 1$. □

7.3.2 Les nombres de Catalan

Définition 7.20 (Nombres de Catalan)**.** Les **nombres de Catalan** $(C_n)_{n\geq 0}$ sont définis par $C_0 = 1$ et la récurrence

$$C_{n+1} = \sum_{i=0}^{n} C_i \, C_{n-i}, \qquad n \geq 0. \tag{7.3}$$

Les premiers termes sont : $1, 1, 2, 5, 14, 42, 132, 429, \ldots$

Théorème 7.21 (Forme close des nombres de Catalan)**.** *Pour tout $n \geq 0$,*

$$C_n = \frac{1}{n+1}\binom{2n}{n}.$$

Démonstration. Soit $C(x) = \sum_{n\geq 0} C_n x^n$ la série génératrice des nombres de Catalan. La récurrence (7.3) signifie que le coefficient de x^{n+1} dans $C(x)$ vaut la convolution des coefficients, c'est-à-dire

$$C(x) = 1 + x\,C(x)^2.$$

En résolvant cette équation quadratique en $C(x)$:

$$C(x) = \frac{1 - \sqrt{1-4x}}{2x}$$

(on choisit la racine donnant $C(0) = 1$). En développant $\sqrt{1-4x}$ par la formule du binôme généralisé $\sqrt{1-4x} = \sum_{n=0}^{\infty} \binom{1/2}{n}(-4x)^n$ et en identifiant les coefficients, on obtient $C_n = \frac{1}{n+1}\binom{2n}{n}$. □

Exemple 7.22 (Interprétations combinatoires de C_n)**.** Le nombre de Catalan C_n compte, entre autres :

(i) le nombre de parenthésages corrects de n paires de parenthèses ;

(ii) le nombre d'arbres binaires complets à n nœuds internes ;

(iii) le nombre de chemins de Dyck de longueur $2n$ (chemins monotones de $(0,0)$ à $(2n,0)$ par pas $(1,1)$ et $(1,-1)$ ne passant jamais sous l'axe des abscisses) ;

(iv) le nombre de triangulations d'un polygone convexe à $(n+2)$ sommets.

7.4 Récurrences de type diviser pour régner

De nombreux algorithmes suivent le paradigme *diviser pour régner* : on divise un problème de taille n en a sous-problèmes de taille n/b, puis on combine les résultats en temps $\Theta(n^d)$.

Définition 7.23 (Récurrence de diviser pour régner)**.** Une récurrence de la forme

$$T(n) = a\,T(n/b) + f(n), \tag{7.4}$$

avec $a \geq 1$, $b > 1$ et f une fonction positive, est appelée **récurrence de diviser pour régner**.

Théorème 7.24 (Théorème maître)**.** *Soit* $T(n) = a\,T(n/b) + \Theta(n^d)$ *avec* $a \geq 1$, $b > 1$, $d \geq 0$. *Posons* $c = \log_b a$. *Alors :*

$$T(n) = \begin{cases} \Theta(n^d) & \text{si } d > c, \\ \Theta(n^d \log n) & \text{si } d = c, \\ \Theta(n^c) & \text{si } d < c. \end{cases}$$

Remarque 7.25. Intuitivement, on compare le coût de la combinaison (n^d) au nombre de feuilles de l'arbre de récursion $(a^{\log_b n} = n^{\log_b a} = n^c)$. Si le coût de combinaison domine $(d > c)$, $T(n) = \Theta(n^d)$. Si les feuilles dominent $(d < c)$, $T(n) = \Theta(n^c)$. Si les deux sont équilibrés $(d = c)$, on accumule un facteur logarithmique.

Exemple 7.26 (Tri par fusion)**.** Le tri par fusion satisfait $T(n) = 2T(n/2) + \Theta(n)$, soit $a = 2$, $b = 2$, $d = 1$. On a $c = \log_2 2 = 1 = d$, donc $T(n) = \Theta(n \log n)$.

Exemple 7.27 (Recherche binaire)**.** La recherche binaire satisfait $T(n) = T(n/2) + \Theta(1)$, soit $a = 1$, $b = 2$, $d = 0$. On a $c = \log_2 1 = 0 = d$, donc $T(n) = \Theta(\log n)$.

Exemple 7.28 (Multiplication de Karatsuba)**.** L'algorithme de Karatsuba satisfait $T(n) = 3T(n/2) + \Theta(n)$, soit $a = 3$, $b = 2$, $d = 1$. On a $c = \log_2 3 \approx 1{,}585 > 1 = d$, donc $T(n) = \Theta(n^{\log_2 3})$.

Exemple 7.29 (Multiplication matricielle de Strassen)**.** L'algorithme de Strassen satisfait $T(n) = 7T(n/2) + \Theta(n^2)$, soit $a = 7$, $b = 2$, $d = 2$. On a $c = \log_2 7 \approx 2{,}807 > 2 = d$, donc $T(n) = \Theta(n^{\log_2 7})$.

7.5 Résolution par fonctions génératrices

Les fonctions génératrices (voir chapitre 6) fournissent un outil puissant et systématique pour résoudre les récurrences. La méthode se décompose en trois étapes.

Étape 1. **Traduire** la récurrence en une équation pour la série génératrice $A(x) = \sum_{n\geq 0} a_n x^n$.

Étape 2. **Résoudre** l'équation algébrique (ou fonctionnelle) en $A(x)$.

Étape 3. **Extraire** les coefficients de $A(x)$ par décomposition en fractions partielles ou développement en série.

Exemple 7.30 (Fibonacci par fonctions génératrices)**.** Soit $F(x) = \sum_{n\geq 0} F_n x^n$. La récurrence $F_n = F_{n-1} + F_{n-2}$ (pour $n \geq 2$) avec $F_0 = 0$, $F_1 = 1$ se traduit par :

$$F(x) - F_0 - F_1 x = x\big(F(x) - F_0\big) + x^2 F(x),$$

soit $F(x) - x = xF(x) + x^2F(x)$. D'où

$$F(x) = \frac{x}{1 - x - x^2}.$$

En décomposant en fractions partielles avec $1 - x - x^2 = -(x - \varphi^{-1})(x - \psi^{-1})$ (en notant que $-1/\varphi = \psi$ et $-1/\psi = \varphi$ ne sont pas les racines directes du dénominateur, mais $1/\varphi$ et $1/\psi$ le sont en inversant), on retrouve la formule de Binet.

Exemple 7.31 (Récurrence $a_n = 3a_{n-1} + 2$ par fonctions génératrices)**.** Soit $a_0 = 1$ et $a_n = 3a_{n-1} + 2$ pour $n \geq 1$. Posons $A(x) = \sum_{n\geq 0} a_n x^n$. Alors

$$A(x) - 1 = 3x\, A(x) + \frac{2x}{1 - x}.$$

D'où

$$A(x) = \frac{1 - x + 2x}{(1 - x)(1 - 3x)} = \frac{1 + x}{(1 - x)(1 - 3x)}.$$

Par fractions partielles : $A(x) = \frac{-1}{1-x} + \frac{2}{1-3x}$, d'où $a_n = -1 + 2 \cdot 3^n = 2 \cdot 3^n - 1$.
Vérification : $a_0 = 2 - 1 = 1$, $a_1 = 6 - 1 = 5 = 3 \cdot 1 + 2$. ✓

7.6 Exercices

Exercice 7.1 (Récurrence d'ordre 2)**.** Résoudre les récurrences suivantes avec les conditions initiales données :

(a) $a_n = 7a_{n-1} - 10a_{n-2}$, $\quad a_0 = 2$, $a_1 = 1$.

(b) $a_n = 6a_{n-1} - 9a_{n-2}$, $\quad a_0 = 1$, $a_1 = 6$.

(c) $a_n = -2a_{n-1} - a_{n-2}$, $\quad a_0 = 0$, $a_1 = 1$.

Exercice 7.2 (Récurrences non homogènes)**.** Résoudre les récurrences suivantes :

(a) $a_n = 2a_{n-1} + 3$, $\quad a_0 = 1$.

(b) $a_n = 3a_{n-1} + n$, $\quad a_0 = 0$.

(c) $a_n = 2a_{n-1} + 3^n, \quad a_0 = 1.$

(d) $a_n = 4a_{n-1} - 4a_{n-2} + 2^n, \quad a_0 = 0,\ a_1 = 1.$

Exercice 7.3 (Identités de Fibonacci)**.** Montrer les identités suivantes pour la suite de Fibonacci :

(a) $\sum_{k=0}^{n} F_k = F_{n+2} - 1.$

(b) $\sum_{k=0}^{n} F_k^2 = F_n\, F_{n+1}.$

(c) $F_{m+n} = F_{m-1}\, F_n + F_m\, F_{n+1}$ pour $m \geq 1.$

(d) $\text{pgcd}(F_m, F_n) = F_{\text{pgcd}(m,n)}.$

Exercice 7.4 (Théorème maître)**.** Utiliser le théorème maître pour déterminer l'ordre de grandeur asymptotique de $T(n)$ dans chacun des cas suivants :

(a) $T(n) = 4T(n/2) + n.$

(b) $T(n) = 4T(n/2) + n^2.$

(c) $T(n) = 4T(n/2) + n^3.$

(d) $T(n) = 8T(n/2) + n^2.$

(e) $T(n) = 2T(n/4) + \sqrt{n}.$

Exercice 7.5 (Suite de Lucas)**.** La **suite de Lucas** est définie par $L_0 = 2$, $L_1 = 1$ et $L_n = L_{n-1} + L_{n-2}$.

(a) Trouver la forme close de L_n.

(b) Montrer que $L_n = F_{n-1} + F_{n+1}$ pour $n \geq 1.$

(c) Montrer que $F_{2n} = F_n L_n.$

Exercice 7.6 (Problème des régions du plan)**.** Soit R_n le nombre maximal de régions créées dans le plan par n droites en position générale (pas deux parallèles, pas trois concourantes).

(a) Montrer que $R_n = R_{n-1} + n$ avec $R_0 = 1.$

(b) En déduire que $R_n = \binom{n}{2} + n + 1 = \frac{n^2+n+2}{2}.$

Exercice 7.7 (Fonctions génératrices et récurrences)**.** Résoudre par la méthode des fonctions génératrices :

(a) $a_n = 5a_{n-1} - 6a_{n-2}$ avec $a_0 = 2,\ a_1 = 5.$

(b) $a_n = a_{n-1} + 2a_{n-2}$ avec $a_0 = 0,\ a_1 = 1.$

Exercice 7.8 (Nombres de Catalan)**.** (a) Vérifier que $C_4 = 14$ en énumérant les parenthésages de 4 paires de parenthèses.

(b) Montrer que $C_n = \frac{4n-2}{n+1}\, C_{n-1}$ pour $n \geq 1.$

(c) Montrer que $C_n \sim \frac{4^n}{n^{3/2}\sqrt{\pi}}$ quand $n \to \infty.$

Résumé du chapitre

— Une **récurrence linéaire homogène** d'ordre k se résout via son **équation caractéristique** : racines distinctes $\to$ combinaison de puissances ; racines répétées $\to$ on multiplie par des polynômes en n.

— Pour une récurrence **non homogène**, la solution générale est la somme de la solution homogène et d'une solution particulière, trouvée par la **méthode des coefficients indéterminés**.

— La **formule de Binet** donne la forme close de la suite de Fibonacci : $F_n = (\varphi^n - \psi^n)/\sqrt{5}$.

— Les **tours de Hanoï** nécessitent $2^n - 1$ déplacements ; les **nombres de Catalan** valent $C_n = \frac{1}{n+1}\binom{2n}{n}$.

— Le **théorème maître** résout les récurrences de diviser pour régner $T(n) = aT(n/b) + \Theta(n^d)$ en comparant d à $\log_b a$.

— Les **fonctions génératrices** offrent une méthode systématique : traduire la récurrence en équation algébrique, résoudre, puis extraire les coefficients.

Chapitre 8

Théorie des Graphes — Notions de Base

Contents

Introduction

La théorie des graphes est l'une des branches les plus vibrantes et les plus applicables des mathématiques discrètes. Née d'un problème récréatif posé par Euler au XVIII^{e} siècle, elle est devenue un outil fondamental en informatique, en recherche opérationnelle, en biologie computationnelle et dans bien d'autres domaines.

8.1 Perspective historique : les ponts de Königsberg

En 1736, Leonhard Euler résolut le célèbre *problème des ponts de Königsberg* : est-il possible de traverser chacun des sept ponts de la ville exactement une fois et de revenir au

point de départ ? Euler montra que c'est impossible et, ce faisant, posa les fondements de la théorie des graphes.

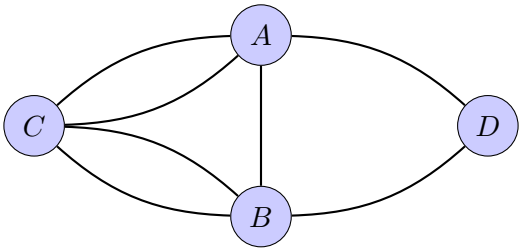


FIGURE 8.1 – Le multigraphe des ponts de Königsberg : chaque sommet représente une masse terrestre, chaque arête un pont.

L'argument d'Euler repose sur une observation simple : pour qu'un tel parcours (appelé aujourd'hui *circuit eulérien*) existe, chaque sommet doit avoir un degré pair, ce qui n'est le cas d'aucun sommet dans le graphe de Königsberg.

8.2 Définitions fondamentales

Définition 8.1 (Graphe simple)**.** Un **graphe simple** (ou simplement un **graphe**) est un couple $G = (V, E)$ où :

- V est un ensemble fini non vide dont les éléments sont appelés **sommets** (ou *nœuds*) ;
- $E \subseteq \binom{V}{2} = \{\{u, v\} : u, v \in V,\ u \neq v\}$ est un ensemble de paires non ordonnées de sommets distincts, appelées **arêtes**.

Notation 8.2. On note $|V| = n$ le **nombre de sommets** (ou *ordre*) et $|E| = m$ le **nombre d'arêtes** (ou *taille*) du graphe.

Définition 8.3 (Adjacence et incidence)**.** Soit $G = (V, E)$ un graphe et $e = \{u, v\} \in E$ une arête.

- Les sommets u et v sont dits **adjacents** (ou *voisins*).
- L'arête e est **incidente** aux sommets u et v.
- On note $N(v) = \{u \in V : \{u, v\} \in E\}$ le **voisinage** de v.

8.2.1 Variantes de graphes

Définition 8.4 (Multigraphe)**.** Un **multigraphe** est un graphe dans lequel on autorise :

- les **arêtes multiples** (plusieurs arêtes entre la même paire de sommets) ;
- les **boucles** (arêtes reliant un sommet à lui-même).

Formellement, E est un multi-ensemble de paires (non nécessairement distinctes) d'éléments de V.

Définition 8.5 (Graphe orienté)**.** Un **graphe orienté** (ou **digraphe**) est un couple $G = (V, A)$ où $A \subseteq V \times V$ est un ensemble de couples ordonnés, appelés **arcs**. Un arc (u, v) va de u (origine) à v (extrémité).

Définition 8.6 (Graphe pondéré)**.** Un **graphe pondéré** est un graphe $G = (V, E)$ muni d'une fonction de poids $w \colon E \to \mathbb{R}$ qui attribue un poids (ou coût) à chaque arête.

8.3 Représentations d'un graphe

8.3.1 Matrice d'adjacence

Définition 8.7 (Matrice d'adjacence)**.** Soit $G = (V, E)$ un graphe simple avec $V = \{v_1, \ldots, v_n\}$. La **matrice d'adjacence** de G est la matrice $A \in \{0, 1\}^{n \times n}$ définie par

$$A_{ij} = \begin{cases} 1 & \text{si } \{v_i, v_j\} \in E, \\ 0 & \text{sinon.} \end{cases}$$

Remarque 8.8. Pour un graphe simple, A est symétrique ($A_{ij} = A_{ji}$) et à diagonale nulle ($A_{ii} = 0$). L'espace mémoire est $\Theta(n^2)$. La matrice d'adjacence est efficace pour tester l'existence d'une arête en $O(1)$, mais coûteuse en mémoire pour les graphes creux.

Exemple 8.9. La matrice d'adjacence du graphe complet K_4 est

$$A = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}.$$

8.3.2 Listes d'adjacence

Définition 8.10 (Liste d'adjacence)**.** La **représentation par listes d'adjacence** d'un graphe $G = (V, E)$ consiste à associer à chaque sommet $v \in V$ la liste de ses voisins $N(v)$.

Remarque 8.11. L'espace mémoire est $\Theta(n + m)$. Cette représentation est préférable pour les graphes creux ($m \ll n^2$), qui sont les plus fréquents en pratique.

8.3.3 Matrice d'incidence

Définition 8.12 (Matrice d'incidence)**.** Soit $G = (V, E)$ un graphe avec $V = \{v_1, \ldots, v_n\}$ et $E = \{e_1, \ldots, e_m\}$. La **matrice d'incidence** $B \in \{0,1\}^{n \times m}$ est définie par

$$B_{ij} = \begin{cases} 1 & \text{si le sommet } v_i \text{ est incident à l'arête } e_j, \\ 0 & \text{sinon.} \end{cases}$$

Remarque 8.13. Chaque colonne de B contient exactement deux 1 (les deux extrémités de l'arête correspondante). La somme de la ligne i donne le degré de v_i.

8.4 Degré d'un sommet

Définition 8.14 (Degré)**.** Le **degré** d'un sommet v dans un graphe $G = (V, E)$, noté $\deg(v)$, est le nombre d'arêtes incidentes à v :

$$\deg(v) = |N(v)| = \operatorname{card}\{e \in E : v \in e\}.$$

Un sommet de degré 0 est dit **isolé**, un sommet de degré 1 est une **feuille** (ou sommet pendant).

Définition 8.15 (Degré dans un graphe orienté)**.** Dans un digraphe $G = (V, A)$, on distingue :

- le **degré entrant** de v : $\deg^-(v) = \operatorname{card}\{u \in V : (u, v) \in A\}$;
- le **degré sortant** de v : $\deg^+(v) = \operatorname{card}\{u \in V : (v, u) \in A\}$.

Théorème 8.16 (Lemme des poignées de main)**.** *Soit $G = (V, E)$ un graphe. Alors*

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

Démonstration. Chaque arête $e = \{u, v\}$ contribue exactement 1 au degré de u et 1 au degré de v. Donc, en sommant les degrés de tous les sommets, chaque arête est comptée exactement deux fois.

Formellement, on peut écrire

$$\sum_{v \in V} \deg(v) = \sum_{v \in V} \sum_{e \in E} \mathbf{1}_{v \in e} = \sum_{e \in E} \sum_{v \in V} \mathbf{1}_{v \in e} = \sum_{e \in E} 2 = 2\,|E|. \qquad \square$$

Corollaire 8.17. *Dans tout graphe, le nombre de sommets de degré impair est pair.*

Démonstration. Séparons les sommets en deux ensembles : V_{pair} (sommets de degré pair)

et V_{impair} (sommets de degré impair). Alors

$$2\,|E| = \sum_{v \in V_{\text{pair}}} \deg(v) + \sum_{v \in V_{\text{impair}}} \deg(v).$$

Le membre de gauche est pair, et la première somme du membre de droite est pair (somme de nombres pairs). Donc la seconde somme est pair. Comme chaque terme de cette somme est impair, le nombre de termes doit être pair. □

Exemple 8.18. Dans le graphe de Königsberg (figure 8.1), les degrés sont : $\deg(A) = 3$, $\deg(B) = 3$, $\deg(C) = 4$, $\deg(D) = 2$ (dans le cas d'un multigraphe à 7 arêtes : $3+3+4+2 \neq 14$). En fait, avec les 7 ponts : $\deg(A) = 3$, $\deg(B) = 3$, $\deg(C) = 3$, $\deg(D) = 5$ dans la version historique originale. La somme des degrés est $3+3+3+5 = 14 = 2 \times 7$.
Remarque : comme les quatre sommets ont tous un degré impair, aucun circuit eulérien n'existe.

8.5 Chemins, cycles et connexité

Définition 8.19 (Marche, chemin, cycle)**.** Soit $G = (V, E)$ un graphe.

- Une **marche** de longueur k est une suite $v_0, e_1, v_1, e_2, \ldots, e_k, v_k$ alternant sommets et arêtes, où $e_i = \{v_{i-1}, v_i\} \in E$ pour tout i. On la note souvent $v_0 v_1 \cdots v_k$.
- Un **chemin** (ou *chaîne élémentaire*) est une marche dont tous les sommets sont distincts.
- Un **cycle** (ou *circuit élémentaire*) est une marche fermée ($v_0 = v_k$) de longueur $k \geq 3$ dont tous les sommets intermédiaires sont distincts.

Définition 8.20 (Connexité)**.** Un graphe $G = (V, E)$ est **connexe** si, pour toute paire de sommets $u, v \in V$, il existe un chemin de u à v dans G.

Définition 8.21 (Composantes connexes)**.** Les **composantes connexes** d'un graphe G sont les sous-graphes connexes maximaux de G. Formellement, ce sont les classes d'équivalence de la relation « être relié par un chemin », qui est une relation d'équivalence sur V.

Proposition 8.22. *La relation $u \sim v$ définie par « il existe un chemin de u à v » est une relation d'équivalence sur V.*

Démonstration. Réflexivité : le chemin de longueur 0 relie v à lui-même. *Symétrie* : si $v_0 v_1 \cdots v_k$ est un chemin de u à v, alors $v_k v_{k-1} \cdots v_0$ est un chemin de v à u. *Transitivité* : si un chemin relie u à v et un autre v à w, leur concaténation contient une marche de u à w, et toute marche contient un chemin (en supprimant les boucles). □

Proposition 8.23. *Un graphe connexe d'ordre n possède au moins $n-1$ arêtes.*

Démonstration. Par récurrence sur n. Pour $n = 1$, $m \geq 0 = n - 1$. Supposons $n \geq 2$ et soit v un sommet de G. Le graphe $G - v$ a au plus $\deg(v)$ composantes connexes (chacune devait être reliée à v). Pour que G soit connexe, il faut au moins une arête entre v et chaque composante. Par hypothèse de récurrence, les composantes de $G - v$ (ayant au total $n - 1$ sommets) nécessitent au moins $(n - 1) -$ (nombre de composantes) arêtes en tout. En ajoutant les arêtes incidentes à v, on obtient $m \geq (n - 1 - c) + c = n - 1$ où c est le nombre de composantes de $G - v$. □

Définition 8.24 (Distance dans un graphe)**.** La **distance** entre deux sommets u et v dans un graphe G, notée $d(u, v)$, est la longueur du plus court chemin de u à v. Si aucun chemin n'existe, on pose $d(u, v) = +\infty$.

8.6 Isomorphisme de graphes

Définition 8.25 (Isomorphisme)**.** Deux graphes $G_1 = (V_1, E_1)$ et $G_2 = (V_2, E_2)$ sont **isomorphes**, noté $G_1 \simeq G_2$, s'il existe une bijection $\varphi \colon V_1 \to V_2$ telle que

$$\{u, v\} \in E_1 \iff \{\varphi(u), \varphi(v)\} \in E_2.$$

Une telle bijection est appelée un **isomorphisme**.

Remarque 8.26. Deux graphes isomorphes ont nécessairement :

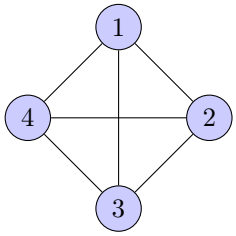
- le même nombre de sommets et le même nombre d'arêtes ;
- la même suite des degrés (triée) ;
- le même nombre de composantes connexes ;
- les mêmes longueurs de cycles.

Ces conditions sont nécessaires mais non suffisantes.

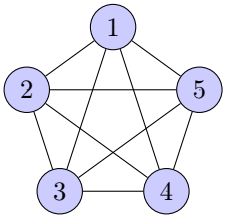
8.7 Familles classiques de graphes

8.7.1 Graphes complets

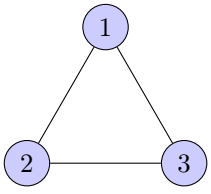
Définition 8.27 (Graphe complet K_n)**.** Le **graphe complet** K_n est le graphe simple sur n sommets dans lequel chaque paire de sommets distincts est reliée par une arête. Il possède $\binom{n}{2} = \frac{n(n-1)}{2}$ arêtes.



K_4



K_5



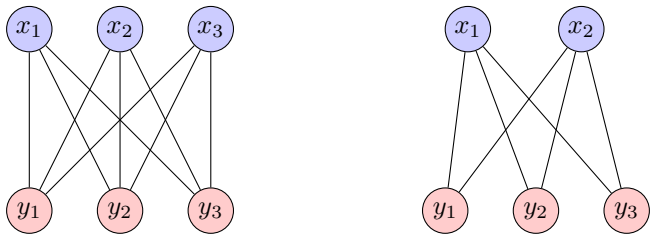
K_3

FIGURE 8.2 – Les graphes complets K_3, K_4 et K_5.

8.7.2 Graphes bipartis

Définition 8.28 (Graphe biparti)**.** Un graphe $G = (V, E)$ est **biparti** s'il existe une partition $V = X \sqcup Y$ telle que toute arête de E relie un sommet de X à un sommet de Y.

Définition 8.29 (Graphe biparti complet $K_{m,n}$)**.** Le **graphe biparti complet** $K_{m,n}$ est le graphe biparti avec $|X| = m$, $|Y| = n$, et toute paire $(x, y) \in X \times Y$ est reliée. Il possède mn arêtes.



$K_{3,3}$ $K_{2,3}$

FIGURE 8.3 – Les graphes bipartis complets $K_{3,3}$ et $K_{2,3}$.

Proposition 8.30 (Caractérisation des graphes bipartis)**.** *Un graphe est biparti si et seulement s'il ne contient aucun cycle de longueur impaire.*

Démonstration. ($\Rightarrow$) Dans un graphe biparti avec partition $V = X \sqcup Y$, tout cycle alterne entre X et Y, donc sa longueur est paire.

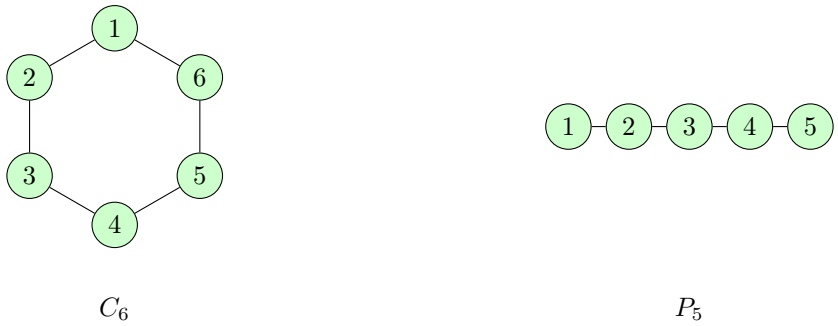
($\Leftarrow$) Supposons que G est connexe et ne contient aucun cycle impair. Fixons un sommet s et posons $X = \{v : d(s, v) \text{ pair}\}$ et $Y = \{v : d(s, v) \text{ impair}\}$. Si une arête $\{u, v\}$ reliait deux sommets de X (resp. de Y), un plus court chemin de s à u, l'arête $\{u, v\}$, et un plus court chemin de v à s formeraient un cycle de longueur $d(s, u) + 1 + d(s, v)$, qui serait impaire puisque $d(s, u)$ et $d(s, v)$ ont même parité. Contradiction. □

8.7.3 Graphes cycles et chemins

Définition 8.31 (Graphe cycle C_n et graphe chemin P_n)**.**

— Le **graphe cycle** C_n ($n \geq 3$) a pour sommets $\{v_1, \ldots, v_n\}$ et pour arêtes $\{v_1v_2, v_2v_3, \ldots, v_{n-1}v_n, v_nv_1\}$. Chaque sommet est de degré 2.

— Le **graphe chemin** P_n ($n \geq 1$) a pour sommets $\{v_1, \ldots, v_n\}$ et pour arêtes $\{v_1v_2, v_2v_3, \ldots, v_{n-1}v_n\}$. Les sommets extrêmes sont de degré 1, les autres de degré 2.



C_6 P_5

FIGURE 8.4 – Le graphe cycle C_6 et le graphe chemin P_5.

8.8 Sous-graphes

Définition 8.32 (Sous-graphe)**.** Un graphe $H = (V', E')$ est un **sous-graphe** de $G = (V, E)$ si $V' \subseteq V$ et $E' \subseteq E$.

Définition 8.33 (Sous-graphe induit)**.** Le **sous-graphe induit** par un sous-ensemble $S \subseteq V$, noté $G[S]$, est le graphe (S, E_S) où $E_S = \{\{u, v\} \in E : u \in S \text{ et } v \in S\}$. Autrement dit, on garde toutes les arêtes de G dont les deux extrémités sont dans S.

Définition 8.34 (Sous-graphe couvrant)**.** Un sous-graphe $H = (V, E')$ de $G = (V, E)$ est dit **couvrant** (ou *engendrant*) si $V' = V$, c'est-à-dire s'il contient tous les sommets de G.

8.9 Le graphe de Petersen

Le **graphe de Petersen** est l'un des graphes les plus importants en théorie des graphes. Il sert fréquemment de contre-exemple et possède de nombreuses propriétés remarquables.

Définition 8.35 (Graphe de Petersen)**.** Le graphe de Petersen a 10 sommets et 15 arêtes. Ses sommets sont les paires $\{i, j\}$ avec $1 \leq i < j \leq 5$, et deux sommets sont adjacents si et seulement si les paires correspondantes sont disjointes.

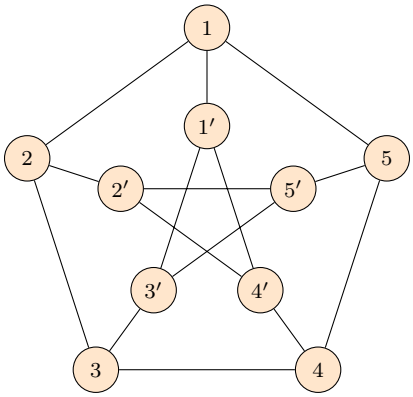


FIGURE 8.5 – Le graphe de Petersen : pentagone extérieur, pentagramme intérieur, et cinq rayons. C'est un graphe 3-régulier avec 10 sommets et 15 arêtes.

Proposition 8.36 (Propriétés du graphe de Petersen)**.** *Le graphe de Petersen satisfait les propriétés suivantes :*

(i) il est 3-régulier (chaque sommet a degré 3) ;

(ii) il est connexe ;

(iii) son diamètre est 2 (la distance maximale entre deux sommets) ;

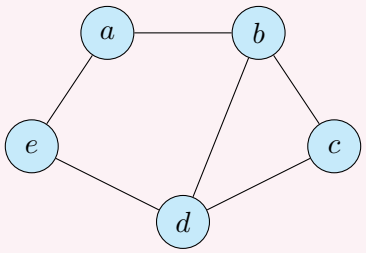
(iv) sa maille est 5 (longueur du plus court cycle) ;

(v) il n'est pas planaire ;

(vi) il n'est pas hamiltonien (il ne possède pas de cycle passant par tous les sommets exactement une fois).

8.10 Quelques illustrations supplémentaires

Exemple 8.37 (Un graphe et ses représentations)**.** Considérons le graphe G suivant :



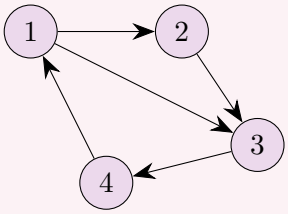
Matrice d'adjacence (avec l'ordre a, b, c, d, e) :

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Listes d'adjacence :

Sommet	Voisins
a	b, e
b	a, c, d
c	b, d
d	b, c, e
e	a, d

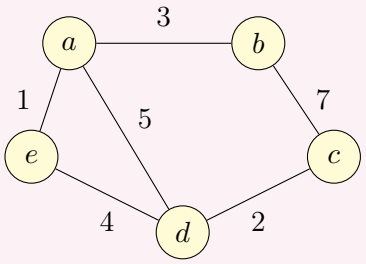
Degrés : $\deg(a) = 2$, $\deg(b) = 3$, $\deg(c) = 2$, $\deg(d) = 3$, $\deg(e) = 2$. Somme : $2 + 3 + 2 + 3 + 2 = 12 = 2 \times 6 = 2m$. ✓



Exemple 8.38 (Graphe orienté)**.**
Ce digraphe a 4 sommets et 5 arcs. Les degrés sont :

Sommet	$\deg^+$	$\deg^-$	$\deg^+ + \deg^-$
1	2	1	3
2	1	1	2
3	1	2	3
4	1	1	2

On vérifie : $\sum \deg^+ = \sum \deg^- = 5 = |A|$.



Exemple 8.39 (Graphe pondéré)**.**

8.11 Exercices

Exercice 8.1 (Dénombrement d'arêtes)**.** (a) Combien d'arêtes possède le graphe complet K_n ?

(b) Combien d'arêtes possède le graphe biparti complet $K_{m,n}$?

(c) Montrer qu'un graphe simple d'ordre n possède au plus $\binom{n}{2}$ arêtes.

Exercice 8.2 (Suites de degrés)**.** Parmi les suites suivantes, lesquelles sont des suites de degrés d'un graphe simple ? Pour celles qui le sont, construire un tel graphe.

(a) $(3, 3, 3, 3)$

(b) $(1, 1, 2, 3, 3)$

(c) $(0, 1, 2, 3)$

(d) $(2, 2, 2, 2, 2)$

(e) $(1, 2, 3, 4, 5)$

Indication : utiliser le théorème d'Erdős–Gallai ou la condition de la somme paire.

Exercice 8.3 (Matrice d'adjacence et chemins)**.** Soit A la matrice d'adjacence d'un graphe G.

(a) Montrer que $(A^k)_{ij}$ est le nombre de marches de longueur k entre v_i et v_j.

(b) En déduire que $\mathrm{tr}(A^2) = 2m$ et que $\mathrm{tr}(A^3)/6$ est le nombre de triangles dans G.

Exercice 8.4 (Graphes bipartis)**.** (a) Le graphe cycle C_n est-il biparti ? Distinguer les cas n pair et n impair.

(b) Montrer que tout arbre est biparti.

(c) Montrer qu'un graphe biparti d'ordre n possède au plus $\lfloor n^2/4 \rfloor$ arêtes.

Exercice 8.5 (Graphe de Petersen)**.** (a) Vérifier que le graphe de Petersen a bien 10 sommets et 15 arêtes.

(b) Montrer que le graphe de Petersen est 3-régulier.

(c) Montrer que le diamètre du graphe de Petersen est 2.

(d) Trouver un cycle de longueur 5 dans le graphe de Petersen et montrer qu'il n'en existe pas de plus court.

Exercice 8.6 (Connexité et suppression d'arêtes)**.** (a) Montrer qu'un graphe connexe d'ordre n et de taille $n-1$ est un arbre.

(b) Montrer que si G est connexe et e est une arête appartenant à un cycle de G, alors $G - e$ est encore connexe.

(c) Une arête e d'un graphe connexe G est un **pont** si $G - e$ n'est pas connexe. Montrer qu'une arête est un pont si et seulement si elle n'appartient à aucun cycle.

Exercice 8.7 (Isomorphisme)**.** Les paires de graphes suivantes sont-elles isomorphes ? Justifier.

(a) C_6 et $K_{3,3}$.

(b) Le graphe cycle C_5 et le graphe complet K_5 privé d'un couplage parfait *(impossible car K_5 a un nombre impair de sommets — interpréter la question comme K_5 privé de deux arêtes non adjacentes).*

(c) Le graphe cube Q_3 (sommets = mots binaires de longueur 3, arêtes entre mots différant d'un bit) et le graphe biparti complet $K_{3,3}$ plus deux arêtes indépendantes.

Exercice 8.8 (Sous-graphes induits)**.** Soit $G = K_5$ et $S = \{1, 2, 3\}$.

(a) Décrire le sous-graphe induit $G[S]$.

(b) Combien de sous-graphes induits (à isomorphisme près) le graphe K_4 possède-t-il ?

(c) Montrer que tout graphe d'ordre $n \geq 3$ contient un sous-graphe induit d'ordre 3 qui est soit K_3, soit le graphe vide sur 3 sommets (théorème de Ramsey pour $R(3,3)$).

Exercice 8.9 (Complément d'un graphe)**.** Le **complément** d'un graphe $G = (V, E)$ est le graphe $\overline{G} = (V, \binom{V}{2} \setminus E)$.

(a) Montrer que $|E(G)| + \left|E(\overline{G})\right| = \binom{n}{2}$.

(b) Montrer que G ou $\overline{G}$ est connexe.

(c) Quel est le complément de C_5 ?

Résumé du chapitre

— Un **graphe simple** $G = (V, E)$ est un ensemble de sommets V relié par des arêtes $E \subseteq \binom{V}{2}$. Les variantes incluent les multigraphes, les digraphes et les graphes pondérés.

— Les principales **représentations** sont la matrice d'adjacence ($\Theta(n^2)$ en espace) et les listes d'adjacence ($\Theta(n+m)$).

— Le **lemme des poignées de main** affirme que $\sum_v \deg(v) = 2m$, ce qui implique que le nombre de sommets de degré impair est pair.

— Un graphe est **connexe** si toute paire de sommets est reliée par un chemin. Les classes d'équivalence de la relation de connexité forment les **composantes connexes**.

— Deux graphes sont **isomorphes** s'il existe une bijection entre leurs sommets préservant l'adjacence.

— Les **familles classiques** incluent le graphe complet K_n ($\binom{n}{2}$ arêtes), le biparti complet $K_{m,n}$ (mn arêtes), le cycle C_n et le chemin P_n.

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

— Le **graphe de Petersen** est un graphe 3-régulier à 10 sommets et 15 arêtes, possédant de nombreuses propriétés remarquables et servant souvent de contre-exemple.

Chapitre 9

Arbres, Graphes Eulériens et Hamiltoniens

9.1 Arbres

Définition 9.1 (Arbre)**.** Un *arbre* est un graphe connexe et acyclique. Un *forêt* est un graphe acyclique (dont chaque composante connexe est un arbre).

Remarque 9.2. Un arbre à n sommets possède exactement $n-1$ arêtes. La réciproque est également vraie sous des hypothèses adéquates, comme le montre le théorème de caractérisation suivant.

Théorème 9.3 (Caractérisation des arbres)**.** *Soit G un graphe à $n \geq 1$ sommets. Les assertions suivantes sont équivalentes :*

(i) G est un arbre (connexe et acyclique).

(ii) G est connexe et possède exactement $n-1$ arêtes.

(iii) G est acyclique et possède exactement $n-1$ arêtes.

(iv) Pour tous sommets u, v de G, il existe un unique chemin de u à v.

(v) G est connexe et la suppression de toute arête le déconnecte.

(vi) G est acyclique et l'ajout de toute arête crée exactement un cycle.

Démonstration. Nous démontrons les implications principales.

(i) ⇒ (ii). Soit G un arbre à n sommets. Procédons par récurrence sur n. Pour $n = 1$, le graphe possède $0 = n-1$ arêtes. Supposons le résultat vrai pour tout arbre à $n-1$ sommets. Puisque G est un arbre à $n \geq 2$ sommets, il possède au moins un sommet pendant v (de degré 1), car sinon tout sommet aurait degré ≥ 2, ce qui impliquerait l'existence d'un cycle (contradiction avec l'acyclicité). Le graphe $G - v$ est encore connexe et acyclique, donc un arbre à $n-1$ sommets ; par hypothèse de récurrence, il possède $n-2$ arêtes. Ainsi G possède $n-2+1 = n-1$ arêtes.

(ii) ⇒ (iii). Supposons G connexe avec $n-1$ arêtes. S'il contenait un cycle C, la suppression d'une arête de C conserverait la connexité, produisant un graphe connexe à $n-1-1 = n-2$ arêtes. On pourrait répéter jusqu'à obtenir un graphe connexe acyclique

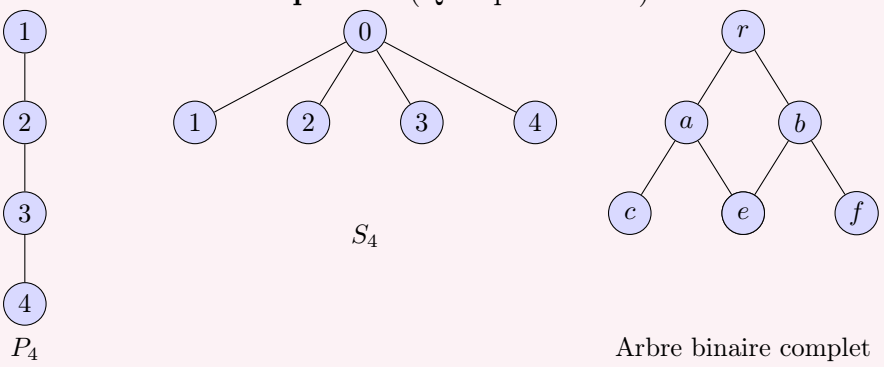
(un arbre) à n sommets avec strictement moins de $n-1$ arêtes. Mais un arbre à n sommets a $n-1$ arêtes (par (i) $\Rightarrow$ (ii)), contradiction.

(iii) $\Rightarrow$ (i). Soit G acyclique avec $n-1$ arêtes. Si G a k composantes connexes, celles-ci sont des arbres de tailles $n_1, \dots, n_k$ avec $\sum n_i = n$. Chaque composante possède $n_i - 1$ arêtes, d'où un total de $n-k$ arêtes. Comme ce total vaut $n-1$, on obtient $k=1$ et G est connexe.

(i) $\Rightarrow$ (iv). La connexité assure l'existence d'un chemin entre toute paire de sommets. S'il existait deux chemins distincts de u à v, leur concaténation contiendrait un cycle, contredisant l'acyclicité.

Les autres implications se démontrent de manière analogue. □

Exemple 9.4 (Quelques arbres)**.**



9.2 Arbres couvrants

Définition 9.5 (Arbre couvrant)**.** Soit $G = (V, E)$ un graphe connexe. Un *arbre couvrant* de G est un sous-graphe couvrant $T = (V, E')$ avec $E' \subseteq E$ qui est un arbre.

Proposition 9.6. *Tout graphe connexe possède au moins un arbre couvrant.*

Démonstration. Soit G connexe. Si G est acyclique, c'est un arbre et il est son propre arbre couvrant. Sinon, G contient un cycle ; on supprime une arête du cycle, ce qui préserve la connexité. On itère jusqu'à obtenir un sous-graphe connexe acyclique couvrant, c'est-à-dire un arbre couvrant. □

Théorème 9.7 (Formule de Cayley)**.** *Le nombre d'arbres couvrants étiquetés du graphe complet K_n est n^{n-2}.*

Exemple 9.8. Pour K_3, la formule donne $3^1 = 3$ arbres étiquetés, ce qui correspond aux trois chemins possibles parmi les sommets $\{1, 2, 3\}$. Pour K_4, on obtient $4^2 = 16$ arbres couvrants étiquetés.

9.3 Arbres couvrants de poids minimum

Définition 9.9 (Graphe pondéré et arbre couvrant de poids minimum)**.** Un *graphe pondéré* est un graphe $G = (V, E)$ muni d'une fonction de poids $w : E \to \mathbb{R}$. Un *arbre couvrant de poids minimum* (ACM) de G est un arbre couvrant dont la somme des poids des arêtes est minimale.

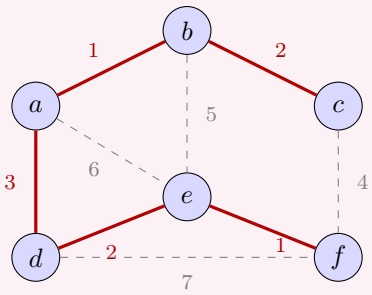
Théorème 9.10 (Algorithme de Kruskal)**.** *L'algorithme suivant produit un ACM d'un graphe connexe pondéré $G = (V, E, w)$ à n sommets :*

1. *Trier les arêtes par poids croissant : $w(e_1) \leq w(e_2) \leq \cdots \leq w(e_m)$.*
2. *Initialiser $T \leftarrow (V, \varnothing)$.*
3. *Pour $i = 1, 2, \ldots, m$: si l'ajout de e_i à T ne crée pas de cycle, ajouter e_i à T.*
4. *Retourner T.*

L'algorithme se termine lorsque T possède $n - 1$ arêtes.

Théorème 9.11 (Algorithme de Prim)**.** *L'algorithme suivant produit un ACM d'un graphe connexe pondéré $G = (V, E, w)$:*

1. *Choisir un sommet initial $s \in V$. Poser $S \leftarrow \{s\}$, $T \leftarrow (S, \varnothing)$.*
2. *Tant que $S \neq V$: parmi les arêtes $\{u, v\}$ avec $u \in S$ et $v \notin S$, choisir celle de poids minimal ; ajouter v à S et l'arête à T.*
3. *Retourner T.*



Exemple 9.12 (Arbre couvrant de poids minimum)**.**
Les arêtes en trait épais forment un ACM de poids total $1 + 2 + 3 + 2 + 1 = 9$.

9.4 Circuits et chemins d'Euler

Définition 9.13 (Chemin et circuit d'Euler)**.** Soit G un graphe (simple ou multigraphe). Un *chemin d'Euler* est un chemin qui emprunte chaque arête exactement une fois. Un *circuit d'Euler* est un chemin d'Euler fermé (le sommet de départ coïncide avec le sommet d'arrivée). Un graphe possédant un circuit d'Euler est dit *eulérien*.

Théorème 9.14 (Condition nécessaire et suffisante pour un circuit d'Euler)**.** *Un multigraphe connexe G possède un circuit d'Euler si et seulement si chaque sommet de G est de degré pair.*

Démonstration. **Condition nécessaire.** Supposons que G possède un circuit d'Euler C. Chaque fois que C traverse un sommet v (distinct du sommet de départ/arrivée), il y entre par une arête et en sort par une autre, contribuant 2 au degré de v. Le sommet de départ/arrivée voit aussi son degré augmenté de 2 à chaque passage. Comme chaque arête est parcourue exactement une fois, le degré de chaque sommet est pair.

Condition suffisante. Supposons que tout sommet de G est de degré pair. On procède par récurrence forte sur le nombre d'arêtes m.

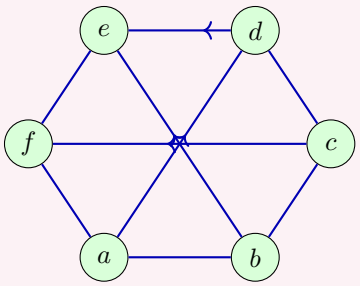
Si $m = 0$, le circuit trivial convient. Supposons $m \geq 1$. Puisque chaque sommet a degré pair ≥ 2 (le graphe étant connexe avec $m \geq 1$), on peut construire une marche fermée W partant d'un sommet quelconque v_0 en suivant des arêtes non encore visitées, sans jamais rester bloqué sur un sommet différent de v_0 (car les degrés pairs garantissent une arête de sortie tant que l'on n'est pas revenu à v_0).

Si W parcourt toutes les arêtes, c'est un circuit d'Euler. Sinon, le graphe $G' = G - E(W)$ a tous ses sommets de degré pair. Chaque composante connexe G'_i de G' ayant un sommet en commun avec W (car G est connexe) possède, par hypothèse de récurrence, un circuit d'Euler C_i. On insère chaque C_i dans W au sommet commun pour obtenir un circuit d'Euler de G. □

Corollaire 9.15 (Condition pour un chemin d'Euler)**.** *Un multigraphe connexe G possède un chemin d'Euler (non fermé) si et seulement si G possède exactement deux sommets de degré impair. Dans ce cas, le chemin relie ces deux sommets.*

Théorème 9.16 (Algorithme de Fleury)**.** *Soit G un multigraphe connexe dont tous les sommets sont de degré pair. L'algorithme suivant produit un circuit d'Euler :*

1. *Partir d'un sommet quelconque v.*
2. *À chaque étape, choisir une arête incidente au sommet courant, en évitant les* ponts *(arêtes dont la suppression déconnecte le graphe restant) sauf s'il n'y a pas d'autre choix.*
3. *Supprimer l'arête choisie et passer au sommet suivant.*
4. *Répéter jusqu'à avoir parcouru toutes les arêtes.*



Exemple 9.17 (Circuit d'Euler)**.**
Ce graphe est eulérien : chaque sommet a degré 4. Un circuit d'Euler possible est

$a \to b \to e \to d \to c \to f \to a \to d \to \cdots$ (en parcourant toutes les arêtes exactement une fois).

9.5 Circuits et chemins hamiltoniens

Définition 9.18 (Chemin et circuit hamiltonien)**.** Un *chemin hamiltonien* d'un graphe G est un chemin qui visite chaque sommet exactement une fois. Un *circuit hamiltonien* est un cycle qui visite chaque sommet exactement une fois. Un graphe possédant un circuit hamiltonien est dit *hamiltonien*.

Remarque 9.19. Contrairement au problème eulérien, il n'existe pas de caractérisation simple des graphes hamiltoniens. Déterminer si un graphe est hamiltonien est un problème NP-complet.

Théorème 9.20 (Théorème de Dirac)**.** *Soit G un graphe simple à $n \geq 3$ sommets. Si $\deg(v) \geq n/2$ pour tout sommet v, alors G est hamiltonien.*

Démonstration. Supposons par l'absurde que G satisfait l'hypothèse mais n'est pas hamiltonien. Ajoutons des arêtes à G de sorte que le graphe résultant G^* ne soit toujours pas hamiltonien, mais que l'ajout de toute arête supplémentaire crée un circuit hamiltonien. Un tel graphe maximal G^* existe.

Soient u et v deux sommets non adjacents dans G^*. L'ajout de $\{u, v\}$ à G^* crée un circuit hamiltonien, donc G^* possède un chemin hamiltonien $v_1 = u, v_2, \ldots, v_n = v$.

Considérons les ensembles :

$$S = \{i : \{u, v_{i+1}\} \in E(G^*)\}, \quad T = \{i : \{v, v_i\} \in E(G^*)\}.$$

On a $S, T \subseteq \{1, \ldots, n-1\}$, $\operatorname{card} S = \deg_{G^*}(u) \geq n/2$ et $\operatorname{card} T = \deg_{G^*}(v) \geq n/2$. Par le principe des tiroirs, $S \cap T \neq \varnothing$, c'est-à-dire il existe un indice i tel que $\{u, v_{i+1}\} \in E(G^*)$ et $\{v, v_i\} \in E(G^*)$.

On obtient alors le circuit hamiltonien :

$$u = v_1, v_2, \ldots, v_i, v, v_{n-1}, v_{n-2}, \ldots, v_{i+1}, u,$$

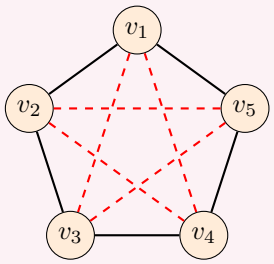
ce qui contredit le choix de G^*. □

Théorème 9.21 (Théorème d'Ore)**.** *Soit G un graphe simple à $n \geq 3$ sommets. Si pour toute paire de sommets non adjacents u, v on a $\deg(u) + \deg(v) \geq n$, alors G est hamiltonien.*

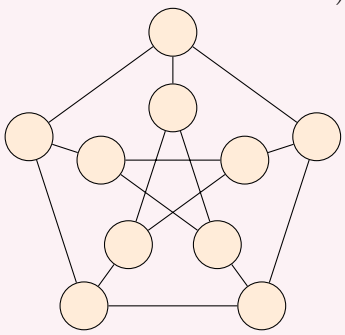
Démonstration. La preuve est identique à celle du théorème de Dirac, en remplaçant la condition $\deg(v) \geq n/2$ par $\deg(u) + \deg(v) \geq n$ pour la paire non adjacente $\{u, v\}$. On obtient de même $\operatorname{card} S + \operatorname{card} T \geq n$ avec $S, T \subseteq \{1, \ldots, n-1\}$, d'où $S \cap T \neq \varnothing$, et la même construction de circuit hamiltonien mène à la contradiction. □

Corollaire 9.22. *Le théorème de Dirac est un cas particulier du théorème d'Ore.*

Exemple 9.23 (Graphe hamiltonien vs non hamiltonien)**.**



C_5 : hamiltonien



Graphe de Petersen
(non hamiltonien)

9.6 Exercices

Exercice 9.1. Montrer qu'un arbre à $n \geq 2$ sommets possède au moins deux sommets pendants (de degré 1).

Exercice 9.2. Déterminer le nombre d'arbres couvrants de K_4 à l'aide de la formule de Cayley, puis les lister explicitement.

Exercice 9.3. Appliquer l'algorithme de Kruskal au graphe complet K_4 avec les poids $w(\{1,2\}) = 3$, $w(\{1,3\}) = 1$, $w(\{1,4\}) = 4$, $w(\{2,3\}) = 5$, $w(\{2,4\}) = 2$, $w(\{3,4\}) = 6$.

Exercice 9.4. Le graphe de Königsberg (les sept ponts) admet-il un chemin d'Euler ? Justifier en calculant les degrés des sommets.

Exercice 9.5. Soit G un graphe simple à $n = 10$ sommets tel que $\deg(v) \geq 5$ pour tout sommet v. Montrer que G est hamiltonien.

Exercice 9.6. Montrer que le graphe de Petersen n'est pas hamiltonien. *Indication : raisonner par l'absurde en considérant un cycle hamiltonien supposé et les arêtes restantes.*

Exercice 9.7. Montrer que tout graphe connexe possède un parcours d'Euler (chemin ou circuit) si et seulement s'il possède au plus deux sommets de degré impair.

Exercice 9.8. Soit T un arbre à n sommets dont les degrés sont $d_1, d_2, \ldots, d_n$. Montrer que $\sum_{i=1}^{n} d_i = 2(n-1)$.

Résumé du chapitre 9. Un arbre est un graphe connexe acyclique ; il possède $n-1$ arêtes et chaque paire de sommets est reliée par un unique chemin. La formule de Cayley dénombre les arbres étiquetés. Les algorithmes de Kruskal et Prim construisent des arbres couvrants de poids minimum. Un graphe connexe est eulérien si et seulement si tous ses sommets sont de degré pair. Les théorèmes de Dirac et d'Ore fournissent des conditions suffisantes pour l'existence de circuits hamiltoniens.

Chapitre 10

Coloration, Planéité et Graphes Bipartis

10.1 Coloration de sommets

Définition 10.1 (Coloration propre et nombre chromatique)**.** Soit $G = (V, E)$ un graphe. Une *coloration propre* de G en k couleurs est une fonction $c : V \to \{1, 2, \ldots, k\}$ telle que $c(u) \neq c(v)$ pour toute arête $\{u, v\} \in E$. Le *nombre chromatique* $\chi(G)$ est le plus petit entier k tel que G admet une coloration propre en k couleurs.

Exemple 10.2. $\chi(K_n) = n$, $\chi(C_{2k}) = 2$, $\chi(C_{2k+1}) = 3$ pour $k \geq 1$.

Proposition 10.3. *Pour tout graphe G, $\chi(G) \leq \Delta(G)+1$, où $\Delta(G) = \max_{v \in V} \deg(v)$.*

Démonstration. L'algorithme glouton suivant réalise cette borne. □

10.1.1 Algorithme de coloration gloutonne

Théorème 10.4 (Coloration gloutonne)**.** *Soit $G = (V, E)$ un graphe à n sommets. L'algorithme suivant produit une coloration propre en au plus $\Delta(G) + 1$ couleurs :*

1. *Numéroter les sommets $v_1, v_2, \ldots, v_n$ dans un ordre quelconque.*
2. *Pour $i = 1, 2, \ldots, n$: attribuer à v_i la plus petite couleur non utilisée par ses voisins déjà colorés.*

Démonstration. Lorsqu'on colore v_i, celui-ci a au plus $\deg(v_i) \leq \Delta(G)$ voisins déjà colorés, occupant au plus $\Delta(G)$ couleurs distinctes. Il reste donc au moins une couleur disponible parmi $\{1, 2, \ldots, \Delta(G) + 1\}$. □

Théorème 10.5 (Théorème de Brooks)**.** *Soit G un graphe connexe qui n'est ni un cycle impair ni un graphe complet. Alors $\chi(G) \leq \Delta(G)$.*

Théorème 10.6 (Théorème des quatre couleurs)**.** *Tout graphe planaire est 4-colorable, c'est-à-dire $\chi(G) \leq 4$ pour tout graphe planaire G.*

Remarque 10.7. Le théorème des quatre couleurs, conjecturé en 1852 par Francis Guthrie, a été démontré en 1976 par Appel et Haken à l'aide d'un programme informatique vérifiant un nombre fini de cas. C'est l'un des premiers théorèmes majeurs dont la preuve repose sur l'assistance d'un ordinateur.

10.2 Polynôme chromatique

Définition 10.8 (Polynôme chromatique)**.** Le *polynôme chromatique* $P(G,k)$ d'un graphe G est le nombre de colorations propres de G en k couleurs.

Proposition 10.9 (Exemples fondamentaux)**.** *(i)* $P(K_n,k) = k(k-1)(k-2)\cdots(k-n+1) = k^{(n)}$ *(factorielle descendante).*

(ii) $P(\overline{K_n},k) = k^n$ *(graphe sans arêtes).*

(iii) $P(T,k) = k(k-1)^{n-1}$ *pour tout arbre T à n sommets.*

Théorème 10.10 (Relation de suppression-contraction)**.** *Pour toute arête $e=\{u,v\}$ d'un graphe G :*

$$P(G,k) = P(G-e,k) - P(G/e,k),$$

où $G-e$ est le graphe obtenu par suppression de e et G/e le graphe obtenu par contraction de e (identification de u et v).

Démonstration. Les colorations propres de $G-e$ se répartissent en deux catégories : celles où $c(u) \neq c(v)$ (qui sont exactement les colorations propres de G) et celles où $c(u) = c(v)$ (qui correspondent bijectivement aux colorations propres de G/e). D'où $P(G-e,k) = P(G,k) + P(G/e,k)$. □

Exemple 10.11 (Calcul de $P(C_4,k)$)**.** En appliquant la relation de suppression-contraction à une arête de C_4 :

$$\begin{aligned} P(C_4,k) &= P(P_4,k) - P(C_3,k) \\ &= k(k-1)^3 - k(k-1)(k-2) \\ &= k(k-1)\big[(k-1)^2 - (k-2)\big] \\ &= k(k-1)(k^2-3k+3). \end{aligned}$$

On retrouve $P(C_4,2) = 2\cdot 1\cdot 1 = 2$ et $P(C_4,3) = 3\cdot 2\cdot 3 = 18$.

10.3 Graphes planaires

Définition 10.12 (Graphe planaire)**.** Un graphe est *planaire* s'il peut être dessiné dans le plan sans croisement d'arêtes. Un tel dessin est appelé une *représentation planaire* ou un *plongement planaire*. Les régions délimitées par les arêtes dans un plongement planaire sont appelées *faces*.

Théorème 10.13 (Formule d'Euler)**.** *Soit G un graphe planaire connexe à V sommets, E arêtes et F faces (y compris la face extérieure). Alors :*

$$V - E + F = 2.$$

Démonstration. Procédons par récurrence sur le nombre d'arêtes E.

Base. Si $E = 0$, alors G est réduit à un sommet ($V = 1$) et possède une seule face ($F = 1$). On a $1 - 0 + 1 = 2$.

Pas de récurrence. Supposons le résultat vrai pour tout graphe planaire connexe à moins de E arêtes, et soit G un graphe planaire connexe à $E \geq 1$ arêtes.

Cas 1 : G contient un cycle. Soit e une arête appartenant à un cycle. L'arête e sépare deux faces distinctes. Le graphe $G - e$ est encore planaire et connexe (car e appartient à un cycle), avec V sommets, $E - 1$ arêtes et $F - 1$ faces (la suppression de e fusionne les deux faces adjacentes). Par hypothèse de récurrence :

$$V - (E - 1) + (F - 1) = 2,$$

d'où $V - E + F = 2$.

Cas 2 : G est acyclique, donc un arbre. Alors $E = V - 1$ et $F = 1$ (la seule face est la face extérieure). On obtient $V - (V - 1) + 1 = 2$. □

Corollaire 10.14. *Pour tout graphe planaire simple connexe à $V \geq 3$ sommets : $E \leq 3V - 6$.*

Démonstration. Chaque face est délimitée par au moins 3 arêtes, et chaque arête borde au plus 2 faces, d'où $2E \geq 3F$. Combiné avec $F = 2 - V + E$ (formule d'Euler), on obtient $2E \geq 3(2 - V + E) = 6 - 3V + 3E$, soit $E \leq 3V - 6$. □

Corollaire 10.15. *Pour tout graphe planaire simple connexe sans triangle à $V \geq 3$ sommets : $E \leq 2V - 4$.*

Démonstration. Sans triangle, chaque face est délimitée par au moins 4 arêtes, d'où $2E \geq 4F$. On conclut de manière analogue. □

Théorème 10.16 (K_5 n'est pas planaire)**.** *Le graphe complet K_5 n'est pas planaire.*

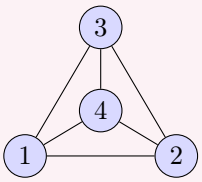
Démonstration. K_5 possède $V = 5$ sommets et $E = \binom{5}{2} = 10$ arêtes. Or $3V - 6 = 9 < 10 = E$, contredisant le corollaire 10.14. □

Théorème 10.17 ($K_{3,3}$ n'est pas planaire)**.** *Le graphe biparti complet $K_{3,3}$ n'est pas planaire.*

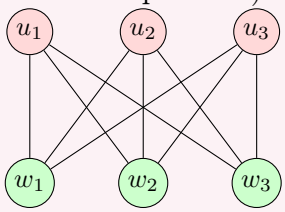
Démonstration. $K_{3,3}$ possède $V = 6$ sommets et $E = 9$ arêtes. Étant biparti, il ne contient aucun cycle de longueur impaire, en particulier pas de triangle. Par le corollaire 10.15, $E \leq 2V - 4 = 8 < 9 = E$, contradiction. □

Théorème 10.18 (Théorème de Kuratowski)**.** *Un graphe est planaire si et seulement s'il ne contient aucun sous-graphe homéomorphe à K_5 ou à $K_{3,3}$.*

Exemple 10.19 (Graphes planaire et non planaire)**.**



K_4 (planaire)



$K_{3,3}$ (non planaire)

10.4 Graphes bipartis

Définition 10.20 (Graphe biparti)**.** Un graphe $G = (V, E)$ est *biparti* s'il existe une partition $V = A \cup B$ ($A \cap B = \varnothing$) telle que toute arête de G relie un sommet de A à un sommet de B. La paire (A, B) est appelée une *bipartition* de G.

Théorème 10.21 (Caractérisation des graphes bipartis)**.** *Un graphe G est biparti si et seulement s'il ne contient aucun cycle de longueur impaire.*

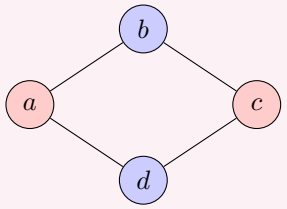
Démonstration. ($\Rightarrow$) Soit G biparti de bipartition (A, B) et soit $C = v_0, v_1, \ldots, v_\ell = v_0$ un cycle dans G. Les sommets de C alternent entre A et B : si $v_0 \in A$, alors $v_1 \in B$, $v_2 \in A$, etc. Puisque $v_\ell = v_0 \in A$, on a ℓ pair. Donc tout cycle est de longueur paire.

($\Leftarrow$) Supposons que G ne contient aucun cycle de longueur impaire. On peut supposer G connexe (sinon, on traite chaque composante séparément). Fixons un sommet s et posons :

$$A = \{v \in V : d(s, v) \text{ est pair}\}, \quad B = \{v \in V : d(s, v) \text{ est impair}\},$$

où $d(s, v)$ est la distance (longueur d'un plus court chemin) de s à v.

Montrons que (A, B) est une bipartition. Soit $\{u, w\} \in E$; nous devons montrer que u et w ne sont pas dans la même partie. Par l'absurde, supposons $u, w \in A$ (le cas B est analogue) avec $d(s, u) = 2p$ et $d(s, w) = 2q$. Soient P_u un plus court chemin de s à u et P_w un plus court chemin de s à w. La concaténation de P_u, de l'arête $\{u, w\}$ et du renversé de P_w donne une marche fermée de longueur $2p + 1 + 2q$, qui est impaire. Cette marche fermée contient un cycle de longueur impaire, contredisant l'hypothèse. □



C_4 : biparti (2-colorable)

Exemple 10.22 (Coloration et bipartition)**.**

10.5 Couplages et théorèmes de König et Hall

Définition 10.23 (Couplage)**.** Un *couplage* dans un graphe $G = (V, E)$ est un ensemble $M \subseteq E$ d'arêtes deux à deux disjointes (sans sommet commun). Un couplage est *maximal* s'il ne peut être étendu, et *maximum* si $\operatorname{card} M$ est maximale. Un couplage *parfait* est un couplage qui couvre tous les sommets.

Définition 10.24 (Couverture par sommets)**.** Une *couverture par sommets* de G est un ensemble $S \subseteq V$ tel que toute arête de G est incidente à au moins un sommet de S.

Théorème 10.25 (Théorème de König)**.** *Dans un graphe biparti, la taille d'un couplage maximum est égale à la taille d'une couverture minimale par sommets.*

Théorème 10.26 (Théorème du mariage de Hall)**.** *Soit G un graphe biparti de bipartition (A, B). Il existe un couplage couvrant tous les sommets de A si et seulement si la* condition de Hall *est satisfaite :*

$$\operatorname{card} N(S) \geq \operatorname{card} S \quad \textit{pour tout } S \subseteq A,$$

où $N(S) = \{b \in B : \exists\, a \in S,\ \{a, b\} \in E\}$ désigne le voisinage de S.

Démonstration. ($\Rightarrow$) Si un couplage M couvre A, alors pour tout $S \subseteq A$, les sommets de S sont appariés à $\operatorname{card} S$ sommets distincts de B appartenant à $N(S)$, d'où $\operatorname{card} N(S) \geq \operatorname{card} S$.

($\Leftarrow$) Procédons par récurrence sur $\operatorname{card} A$.

Base. Si $\operatorname{card} A = 0$ ou $\operatorname{card} A = 1$, le résultat est immédiat.

Pas de récurrence. Supposons $\operatorname{card} A \geq 2$.

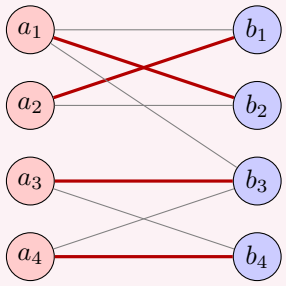
Cas 1 : $\operatorname{card} N(S) \geq \operatorname{card} S + 1$ pour tout $\varnothing \neq S \subsetneq A$. Choisissons un sommet $a \in A$ et un voisin $b \in N(a)$. Le graphe $G' = G - \{a, b\}$ est biparti de bipartition $(A' = A \setminus \{a\},\ B' = B \setminus \{b\})$. Pour tout $S \subseteq A'$ non vide, $\operatorname{card} N_{G'}(S) \geq \operatorname{card} N_G(S) - 1 \geq (\operatorname{card} S + 1) - 1 = \operatorname{card} S$. Par récurrence, G' possède un couplage couvrant A', que l'on

complète par l'arête $\{a, b\}$.

Cas 2 : il existe $\varnothing \neq S_0 \subsetneq A$ tel que $\operatorname{card} N(S_0) = \operatorname{card} S_0$. Par récurrence, le sous-graphe induit par $S_0 \cup N(S_0)$ possède un couplage M_1 couvrant S_0. Posons $A'' = A \setminus S_0$, $B'' = B \setminus N(S_0)$, et considérons le sous-graphe G'' induit par $A'' \cup B''$. Pour tout $S \subseteq A''$, on a :

$$\operatorname{card} N_{G''}(S) = \operatorname{card} N_G(S \cup S_0) - \operatorname{card} N(S_0) \geq \operatorname{card} S \cup S_0 - \operatorname{card} S_0 = \operatorname{card} S.$$

(Si $\operatorname{card} N_{G''}(S) < \operatorname{card} S$, alors $\operatorname{card} N_G(S \cup S_0) < \operatorname{card} S + \operatorname{card} S_0 = \operatorname{card} S \cup S_0$, contradiction avec la condition de Hall.) Par récurrence, G'' possède un couplage M_2 couvrant A''. L'union $M_1 \cup M_2$ couvre A. □



Couplage parfait en rouge

Exemple 10.27 (Couplage dans un graphe biparti)**.**

10.6 Exercices

Exercice 10.1. Calculer le nombre chromatique des graphes suivants : K_6, C_7, $K_{3,3}$, le graphe de Petersen.

Exercice 10.2. Calculer le polynôme chromatique de C_5 par suppression-contraction.

Exercice 10.3. Vérifier la formule d'Euler pour le cube ($V = 8$, $E = 12$, $F = 6$).

Exercice 10.4. Montrer que tout graphe planaire possède un sommet de degré au plus 5. *Indication : utiliser $E \leq 3V - 6$ et la formule des degrés.*

Exercice 10.5. Montrer que le graphe de Petersen n'est pas planaire. *Indication : il contient un sous-graphe homéomorphe à $K_{3,3}$.*

Exercice 10.6. Déterminer le polynôme chromatique du graphe complet biparti $K_{2,3}$.

Exercice 10.7. On considère n filles, chacune connaissant un certain nombre de garçons. Chaque fille connaît au moins k garçons, et chaque garçon est connu d'au plus k filles. Montrer qu'il existe un couplage complet (chaque fille est appariée à un garçon qu'elle connaît). *Indication : vérifier la condition de Hall.*

Exercice 10.8. Un graphe planaire biparti à $V \geq 3$ sommets satisfait $E \leq 2V - 4$. Montrer ce résultat et en déduire que $K_{3,3}$ n'est pas planaire.

Exercice 10.9. Montrer que le polynôme chromatique d'un arbre à n sommets est $P(T,k) = k(k-1)^{n-1}$. *Indication : récurrence en utilisant un sommet pendant.*

Résumé du chapitre 10. Le nombre chromatique $\chi(G)$ est le nombre minimal de couleurs pour une coloration propre. Le théorème de Brooks affine la borne $\Delta(G)+1$. Le polynôme chromatique se calcule par suppression-contraction. La formule d'Euler $V - E + F = 2$ caractérise les plongements planaires et entraîne $E \leq 3V - 6$, ce qui permet de démontrer la non-planarité de K_5 et $K_{3,3}$. Un graphe est biparti si et seulement s'il ne contient pas de cycle impair. Le théorème de Hall donne une condition nécessaire et suffisante pour l'existence d'un couplage complet dans un graphe biparti.

Chapitre 11

Introduction à la Théorie des Codes

11.1 Motivation

Les données numériques — texte, images, sons — sont transmises sous forme de suites de symboles (typiquement des bits 0 et 1) à travers des canaux imparfaits : câbles, ondes radio, supports de stockage. Des erreurs de transmission peuvent altérer les données. La *théorie des codes correcteurs* vise à ajouter de la redondance aux messages de manière structurée, afin de *détecter* et, si possible, *corriger* les erreurs introduites lors de la transmission.

Remarque 11.1. La théorie des codes se situe à l'intersection de l'algèbre linéaire, de la combinatoire et de la théorie de l'information. Elle constitue une application majeure des mathématiques discrètes.

11.2 Alphabet, mots et distance de Hamming

Définition 11.2 (Alphabet et mots)**.** Un *alphabet* est un ensemble fini $\mathcal{A}$ de symboles. Un *mot* de longueur n sur $\mathcal{A}$ est un élément de $\mathcal{A}^n$. Dans ce chapitre, nous travaillons principalement avec l'alphabet binaire $\mathcal{A} = \mathbb{F}_2 = \{0, 1\}$, le corps à deux éléments.

Définition 11.3 (Distance de Hamming)**.** Soient $\mathbf{x} = (x_1, \ldots, x_n)$ et $\mathbf{y} = (y_1, \ldots, y_n)$ deux mots de $\mathcal{A}^n$. La *distance de Hamming* entre $\mathbf{x}$ et $\mathbf{y}$ est :

$$d(\mathbf{x}, \mathbf{y}) = \operatorname{card}\{i : x_i \neq y_i\}.$$

Définition 11.4 (Poids de Hamming)**.** Le *poids de Hamming* d'un mot $\mathbf{x} \in \mathbb{F}_2^n$ est le nombre de composantes non nulles :

$$w(\mathbf{x}) = d(\mathbf{x}, \mathbf{0}) = \operatorname{card}\{i : x_i \neq 0\}.$$

Proposition 11.5. *La distance de Hamming est une métrique sur $\mathcal{A}^n$:*

(i) $d(\mathbf{x}, \mathbf{y}) \geq 0$*, avec égalité si et seulement si* $\mathbf{x} = \mathbf{y}$*.*

(ii) $d(\mathbf{x},\mathbf{y}) = d(\mathbf{y},\mathbf{x})$ *(symétrie).*

(iii) $d(\mathbf{x},\mathbf{z}) \leq d(\mathbf{x},\mathbf{y}) + d(\mathbf{y},\mathbf{z})$ *(inégalité triangulaire).*

Démonstration. Les propriétés (i) et (ii) sont immédiates. Pour (iii), si $x_i \neq z_i$, alors nécessairement $x_i \neq y_i$ ou $y_i \neq z_i$ (ou les deux). Donc chaque position contribuant à $d(\mathbf{x},\mathbf{z})$ contribue à $d(\mathbf{x},\mathbf{y})$ ou $d(\mathbf{y},\mathbf{z})$. □

11.3 Codes détecteurs et correcteurs d'erreurs

Définition 11.6 (Code en bloc)**.** Un *code en bloc* de longueur n et de taille M sur un alphabet $\mathcal{A}$ est un sous-ensemble $C \subseteq \mathcal{A}^n$ avec $\operatorname{card} C = M$. Les éléments de C sont les *mots de code*. La *distance minimale* du code est :

$$d(C) = \min_{\substack{\mathbf{x},\mathbf{y}\in C \\ \mathbf{x}\neq\mathbf{y}}} d(\mathbf{x},\mathbf{y}).$$

On note un tel code un (n, M, d)-code.

Théorème 11.7 (Capacités de détection et de correction)**.** *Un code de distance minimale d peut :*

(i) détecter jusqu'à $d-1$ erreurs ;

(ii) corriger jusqu'à $\lfloor (d-1)/2 \rfloor$ erreurs.

Démonstration. (i) Si au plus $d-1$ erreurs transforment un mot de code $\mathbf{c}$ en un mot $\mathbf{r}$, alors $d(\mathbf{c},\mathbf{r}) \leq d-1 < d$, donc $\mathbf{r}$ n'est pas un mot de code (sinon la distance minimale serait $< d$). L'erreur est donc détectée.

(ii) Posons $t = \lfloor (d-1)/2 \rfloor$. Si $\mathbf{c}$ est envoyé et $\mathbf{r}$ est reçu avec au plus t erreurs, alors $d(\mathbf{c},\mathbf{r}) \leq t$. Pour tout autre mot de code $\mathbf{c}' \neq \mathbf{c}$, par l'inégalité triangulaire : $d \leq d(\mathbf{c},\mathbf{c}') \leq d(\mathbf{c},\mathbf{r}) + d(\mathbf{r},\mathbf{c}')$, d'où $d(\mathbf{r},\mathbf{c}') \geq d - t > t$. Le mot de code le plus proche de $\mathbf{r}$ est donc $\mathbf{c}$. □

Théorème 11.8 (Borne de l'empilement de sphères (borne de Hamming))**.** *Si C est un code binaire (n, M, d) avec $d = 2t+1$, alors :*

$$M \cdot \sum_{i=0}^{t} \binom{n}{i} \leq 2^n.$$

Démonstration. Les boules de rayon t centrées sur les mots de code sont deux à deux disjointes (car la distance entre deux mots de code est $\geq 2t+1$). Chaque boule contient $\sum_{i=0}^{t} \binom{n}{i}$ mots de $\mathbb{F}_2^n$, et l'espace total contient 2^n mots. □

Définition 11.9 (Code parfait)**.** Un code atteignant l'égalité dans la borne de Hamming est appelé *code parfait* : les boules de rayon t centrées sur les mots de code

forment une partition de $\mathbb{F}_2^n$.

11.4 Codes linéaires

Définition 11.10 (Code linéaire)**.** Un *code linéaire* binaire $[n, k, d]$ est un sous-espace vectoriel C de dimension k de $\mathbb{F}_2^n$ dont la distance minimale est d. Le *rendement* (ou *taux*) du code est $R = k/n$.

Proposition 11.11. *Pour un code linéaire, la distance minimale est égale au poids minimal d'un mot de code non nul :*

$$d(C) = \min_{\mathbf{c} \in C \setminus \{\mathbf{0}\}} w(\mathbf{c}).$$

Démonstration. Soient $\mathbf{x}, \mathbf{y} \in C$ distincts. Alors $\mathbf{x} - \mathbf{y} = \mathbf{x} + \mathbf{y} \in C$ (dans $\mathbb{F}_2$, $- = +$) et $d(\mathbf{x}, \mathbf{y}) = w(\mathbf{x} + \mathbf{y})$. Comme $\mathbf{x} + \mathbf{y}$ parcourt tous les mots de code non nuls lorsque $(\mathbf{x}, \mathbf{y})$ parcourt les paires distinctes, le minimum est atteint. □

Définition 11.12 (Matrice génératrice et matrice de contrôle)**.** Soit C un code linéaire $[n, k]$.

- Une *matrice génératrice* de C est une matrice $G \in \mathbb{F}_2^{k \times n}$ dont les lignes forment une base de C. On a $C = \{\mathbf{u}G : \mathbf{u} \in \mathbb{F}_2^k\}$.
- Une *matrice de contrôle* (ou de parité) est une matrice $H \in \mathbb{F}_2^{(n-k) \times n}$ telle que $C = \ker(H) = \{\mathbf{x} \in \mathbb{F}_2^n : H\mathbf{x}^T = \mathbf{0}\}$.

Si $G = [I_k \mid A]$ (forme systématique), alors $H = [-A^T \mid I_{n-k}] = [A^T \mid I_{n-k}]$ (dans $\mathbb{F}_2$).

Théorème 11.13 (Distance minimale et matrice de contrôle)**.** *La distance minimale d d'un code linéaire C de matrice de contrôle H est le plus petit nombre de colonnes de H linéairement dépendantes.*

Démonstration. Un mot $\mathbf{c}$ de poids w appartient à C si et seulement si $H\mathbf{c}^T = \mathbf{0}$, c'est-à-dire si et seulement si la somme des w colonnes de H correspondant aux positions non nulles de $\mathbf{c}$ est nulle. Le poids minimal non nul correspond donc au plus petit nombre de colonnes linéairement dépendantes. □

11.4.1 Décodage par syndrome

Définition 11.14 (Syndrome)**.** Soit H la matrice de contrôle d'un code $[n, k]$ et soit $\mathbf{r}$ un mot reçu. Le *syndrome* de $\mathbf{r}$ est $\mathbf{s} = H\mathbf{r}^T \in \mathbb{F}_2^{n-k}$.

Proposition 11.15. *Le syndrome ne dépend que de l'erreur, pas du mot de code envoyé. Si $\mathbf{r} = \mathbf{c} + \mathbf{e}$ (mot reçu = mot envoyé + erreur), alors $\mathbf{s} = H\mathbf{e}^T$.*

Démonstration. $H\mathbf{r}^T = H(\mathbf{c}+\mathbf{e})^T = H\mathbf{c}^T + H\mathbf{e}^T = \mathbf{0} + H\mathbf{e}^T = H\mathbf{e}^T$. □

Remarque 11.16. Le décodage par syndrome consiste à :

1. calculer $\mathbf{s} = H\mathbf{r}^T$;
2. trouver le vecteur d'erreur $\mathbf{e}$ de poids minimal tel que $H\mathbf{e}^T = \mathbf{s}$ (le *chef de classe*) ;
3. décoder $\hat{\mathbf{c}} = \mathbf{r} - \mathbf{e}$.

11.5 Codes de Hamming

Définition 11.17 (Code de Hamming $\mathrm{Ham}(r,2)$)**.** Pour un entier $r \geq 2$, le *code de Hamming* binaire $\mathrm{Ham}(r,2)$ est le code linéaire $[n,k,3]$ avec $n = 2^r - 1$ et $k = 2^r - 1 - r$, dont la matrice de contrôle H de taille $r \times n$ a pour colonnes tous les vecteurs non nuls de $\mathbb{F}_2^r$.

Théorème 11.18 (Propriétés du code de Hamming)**.** *Le code* $\mathrm{Ham}(r,2)$ *possède les propriétés suivantes :*

(i) Sa distance minimale est $d = 3$.

(ii) Il corrige toute erreur simple (affectant au plus un bit).

(iii) C'est un code parfait.

Démonstration. (i) Les colonnes de H sont toutes distinctes et non nulles, donc deux colonnes ne sont jamais proportionnelles (dans $\mathbb{F}_2$, il n'y a que 0 et 1). Ainsi $d \geq 3$ par le théorème 11.13. De plus, les trois premières colonnes de H (les vecteurs de la base canonique) satisfont une relation de dépendance si $r \geq 2$, par exemple les colonnes correspondant à $(1,0,\ldots,0)^T$, $(0,1,0,\ldots)^T$ et $(1,1,0,\ldots)^T$ sont liées. Donc $d = 3$.

(ii) Découle de $t = \lfloor (3-1)/2 \rfloor = 1$.

(iii) On vérifie la borne de Hamming : $M \cdot (1+n) = 2^k \cdot 2^r = 2^{k+r} = 2^n$, donc l'égalité est atteinte. □

Exemple 11.19 (Code de Hamming $\mathrm{Ham}(3,2)$: le code $[7,4,3]$)**.** La matrice de contrôle est :

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix},$$

dont les colonnes sont les représentations binaires des entiers $1, 2, \ldots, 7$. La matrice génératrice sous forme systématique est :

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Si le mot reçu est $\mathbf{r} = (1,0,1,1,0,1,0)$, le syndrome est $\mathbf{s} = H\mathbf{r}^T = (1,1,0)^T$, qui est la colonne 6 de H. L'erreur est donc en position 6 et le mot corrigé est $(1,0,1,1,0,0,0)$.

11.6 Codes de répétition et codes de parité

Définition 11.20 (Code de répétition)**.** Le *code de répétition* de longueur n est le code $[n, 1, n]$ défini par $C = \{(0, 0, \ldots, 0), (1, 1, \ldots, 1)\}$. Chaque bit d'information est répété n fois.

Remarque 11.21. Le code de répétition corrige $\lfloor (n-1)/2 \rfloor$ erreurs mais a un rendement très faible $R = 1/n$.

Définition 11.22 (Code de parité)**.** Le *code de contrôle de parité* de longueur n est le code $[n, n-1, 2]$ défini par :

$$C = \{(x_1, \ldots, x_n) \in \mathbb{F}_2^n : x_1 + x_2 + \cdots + x_n = 0\}.$$

La matrice de contrôle est $H = (1\ 1\ \cdots\ 1)$.

Remarque 11.23. Le code de parité détecte toute erreur simple ($d = 2$) mais ne corrige aucune erreur. Son rendement $R = (n-1)/n$ est élevé.

Proposition 11.24. *Les codes de répétition et de parité sont duaux l'un de l'autre : le dual du code de répétition $[n, 1, n]$ est le code de parité $[n, n-1, 2]$, et réciproquement.*

11.7 Codes de Reed-Solomon

Remarque 11.25. Les *codes de Reed-Solomon* sont des codes linéaires définis sur des corps finis $\mathbb{F}_q$ (avec $q > 2$ en général). Un code de Reed-Solomon $\mathrm{RS}(n, k)$ sur $\mathbb{F}_q$ a pour paramètres $[n, k, n-k+1]$ avec $n = q - 1$. Il atteint la *borne de Singleton* $d \leq n - k + 1$ et est donc un code MDS (*maximum distance separable*).
Ces codes sont utilisés dans de nombreuses applications pratiques : CD, DVD, codes QR, transmissions spatiales, etc. Leur étude détaillée dépasse le cadre de ce cours d'introduction mais illustre la puissance des méthodes algébriques (polynômes sur les corps finis) en théorie des codes.

11.8 Lien avec les mathématiques discrètes

La théorie des codes fait appel de manière essentielle à plusieurs branches des mathématiques discrètes :

— **Algèbre linéaire sur les corps finis.** Les codes linéaires sont des sous-espaces vectoriels de $\mathbb{F}_q^n$. Les opérations de codage, décodage et détection d'erreurs se ramènent à des calculs matriciels sur $\mathbb{F}_q$.

— **Combinatoire.** Le dénombrement des mots de code de poids donné (distribution des poids) utilise les coefficients binomiaux et les identités combinatoires. Les bornes

fondamentales (Hamming, Singleton, Plotkin, Gilbert-Varshamov) sont de nature combinatoire.

— **Théorie des graphes.** Certains codes sont définis à partir de graphes (codes LDPC, codes de Tanner). Les graphes de Cayley interviennent dans l'analyse de codes algébriques.

— **Théorie des nombres.** Les corps finis $\mathbb{F}_{p^r}$ sont construits à l'aide de polynômes irréductibles sur $\mathbb{F}_p$. Les racines primitives et la structure multiplicative de $\mathbb{F}_q^*$ jouent un rôle central dans la construction des codes BCH et Reed-Solomon.

11.9 Exercices

Exercice 11.1. Calculer la distance de Hamming entre les mots $\mathbf{x} = (1, 0, 1, 1, 0)$ et $\mathbf{y} = (0, 1, 1, 0, 0)$.

Exercice 11.2. Un code binaire C a pour mots de code : $\{00000, 01101, 10110, 11011\}$.

(a) Calculer la distance minimale de C.

(b) Combien d'erreurs C peut-il détecter ? Corriger ?

(c) C est-il linéaire ?

Exercice 11.3. Construire la matrice de contrôle du code de Hamming $\mathrm{Ham}(4, 2)$, c'est-à-dire le code $[15, 11, 3]$. Vérifier que c'est un code parfait.

Exercice 11.4. Soit C le code de Hamming $[7, 4, 3]$ de l'exemple 11.19.

(a) Coder le message $\mathbf{u} = (1, 0, 1, 1)$ en calculant $\mathbf{c} = \mathbf{u}G$.

(b) On reçoit $\mathbf{r} = (1, 1, 1, 1, 0, 0, 1)$. Calculer le syndrome et corriger l'erreur.

Exercice 11.5. Montrer que le code de parité $[n, n-1, 2]$ détecte exactement une erreur mais ne peut en corriger aucune.

Exercice 11.6. Montrer que la borne de Singleton s'écrit $M \leq q^{n-d+1}$ pour un code (n, M, d) sur un alphabet de taille q, c'est-à-dire $d \leq n - k + 1$ pour un code linéaire $[n, k, d]$. *Indication : projeter les mots de code sur $n - d + 1$ coordonnées.*

Exercice 11.7. On souhaite transmettre des messages de 4 bits avec la capacité de corriger 1 erreur. Quel est le nombre minimal de bits de redondance nécessaires ? En déduire que le code de Hamming $[7, 4, 3]$ est optimal pour ces paramètres.

Exercice 11.8. Montrer que le dual d'un code de Hamming $[2^r - 1, 2^r - 1 - r, 3]$ est un code $[2^r - 1, r, 2^{r-1}]$ (code simplexe). Calculer la distribution des poids du code simplexe pour $r = 3$.

Résumé du chapitre 11. La théorie des codes correcteurs d'erreurs associe aux messages une redondance structurée. La distance de Hamming mesure la différence entre mots et détermine les capacités de détection ($d - 1$ erreurs) et de correction ($\lfloor (d-1)/2 \rfloor$ erreurs). Les codes linéaires, décrits par des matrices génératrices et de contrôle, permettent un codage et un décodage efficaces. Les codes de Hamming sont des codes parfaits 1-correcteurs. Cette théorie illustre l'interaction profonde entre algèbre linéaire, combinatoire et théorie des graphes.

Annexe A

Table d'identités combinatoires

Cette annexe rassemble les principales identités combinatoires utilisées dans ce cours et au-delà. Les preuves de la plupart de ces identités figurent dans les chapitres précédents ou peuvent être établies par les méthodes qui y sont développées (récurrence, double comptage, fonctions génératrices).

A.1 Identités sur les coefficients binomiaux

Nom	**Identité**
Symétrie	$\binom{n}{k} = \binom{n}{n-k}$
Absorption	$k\binom{n}{k} = n\binom{n-1}{k-1}$
Formule de Pascal	$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$
Théorème binomial	$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$
Somme d'une ligne	$\sum_{k=0}^{n} \binom{n}{k} = 2^n$
Somme alternée	$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0 \quad (n \geq 1)$
Identité de Vandermonde	$\sum_{k=0}^{r} \binom{m}{k}\binom{n}{r-k} = \binom{m+n}{r}$
Convolution de Vandermonde	$\sum_{k} \binom{r}{k}\binom{s}{n-k} = \binom{r+s}{n}$
Identité du bâton de hockey	$\sum_{i=r}^{n} \binom{i}{r} = \binom{n+1}{r+1}$
Somme des carrés	$\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}$

Nom	**Identité**
Binomiale supérieure	$\sum_{k=0}^{n} \binom{k}{r} = \binom{n+1}{r+1}$
Formule de Chu-Vandermonde	$\sum_{k=0}^{r} \binom{-n}{k}(-1)^k \binom{m}{r-k} = \binom{m+n}{r}$
Double comptage	$\binom{n}{k}\binom{k}{j} = \binom{n}{j}\binom{n-j}{k-j}$

A.2 Nombres de Stirling

Nom / Identité	**Formule**
Stirling 2$^{\text{e}}$ espèce — récurrence	$S(n,k) = k\,S(n-1,k) + S(n-1,k-1)$
Stirling 2$^{\text{e}}$ espèce — formule close	$S(n,k) = \frac{1}{k!}\sum_{j=0}^{k}(-1)^{k-j}\binom{k}{j}j^n$
Nombre de Bell	$B_n = \sum_{k=0}^{n} S(n,k)$
Relation avec les puissances	$x^n = \sum_{k=0}^{n} S(n,k)\,x^{(k)}$
	où $x^{(k)} = x(x-1)\cdots(x-k+1)$
Stirling 1$^{\text{re}}$ espèce — récurrence	$\left[{n \atop k}\right] = (n-1)\left[{n-1 \atop k}\right] + \left[{n-1 \atop k-1}\right]$
Factorielle montante	$x^{(n)} = \sum_{k=0}^{n} \left[{n \atop k}\right](-1)^{n-k}x^k$

A.3 Autres identités remarquables

Nom / Identité	**Formule**
Inclusion-exclusion	$\operatorname{card} A_1 \cup \cdots \cup A_n = \sum_{k=1}^{n}(-1)^{k-1} \sum_{I\subseteq[n],\,\operatorname{card} I=k} \operatorname{card}\bigcap_{i\in I} A_i$
Nombre de surjections	$S(n,k)\cdot k! = \sum_{j=0}^{k}(-1)^{k-j}\binom{k}{j}j^n$

Nom / Identité	**Formule**
Dérangements	$D_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$
Nombres de Catalan	$C_n = \frac{1}{n+1}\binom{2n}{n} = \binom{2n}{n} - \binom{2n}{n+1}$
Récurrence de Catalan	$C_{n+1} = \sum_{i=0}^{n} C_i \, C_{n-i}$
Formule de Cayley	Nombre d'arbres étiquetés sur $[n] = n^{n-2}$
Multinomiale	$(x_1 + \cdots + x_k)^n = \sum_{\substack{n_1+\cdots+n_k=n \\ n_i \geq 0}} \binom{n}{n_1, \ldots, n_k} \prod_{i=1}^{k} x_i^{n_i}$

Remarque A.1. Pour une table plus complète et de nombreuses preuves, on consultera avec profit l'ouvrage de Graham, Knuth et Patashnik [2] ainsi que celui de Cameron [5].

Bibliographie

[1] Rosen, K. H., *Discrete Mathematics and Its Applications*, 8e édition, McGraw-Hill, 2019.

[2] Graham, R. L., Knuth, D. E. et Patashnik, O., *Concrete Mathematics : A Foundation for Computer Science*, 2e édition, Addison-Wesley, 1994.

[3] Lovász, L., Pelikán, J. et Vesztergombi, K., *Discrete Mathematics : Elementary and Beyond*, Springer, 2003.

[4] Diestel, R., *Graph Theory*, 5e édition, Graduate Texts in Mathematics 173, Springer, 2017.

[5] Cameron, P. J., *Combinatorics : Topics, Techniques, Algorithms*, Cambridge University Press, 1994.

[6] van Lint, J. H. et Wilson, R. M., *A Course in Combinatorics*, 2e édition, Cambridge University Press, 2001.

[7] Grimaldi, R. P., *Discrete and Combinatorial Mathematics : An Applied Introduction*, 5e édition, Pearson, 2004.

[8] Bondy, J. A. et Murty, U. S. R., *Graph Theory*, Graduate Texts in Mathematics 244, Springer, 2008.

[9] Hill, R., *A First Course in Coding Theory*, Oxford University Press, 1986.

[10] Roman, S., *Introduction to Coding and Information Theory*, Springer, 1997.

Index