SINF1250 - Mathématiques pour l'informatique

Jerome Thiry

21 mai 2015

Table des matières

Première partie

Logiques et preuves

1 Logique propositionnelle

1.1 Propositions

Définition 1. Proposition : phrase déclarative qui est soit vraie, soit fausse.

La proposition qui est toujours vraie se note T, celle qui est toujours fausse se note F.

1.2 Connecteurs

Il y a moyen de composer des propositions grâce aux opérateurs :
- $\neg$ (négation) ;
- $\wedge$ (conjonction) ;
- $\vee$ (disjonction) ;
- $\rightarrow$ (implication) : p $\rightarrow$ q se lit “si p, alors q” ;
- $\leftrightarrow$ (biconditionnelle) : p $\leftrightarrow$ p se lit “p si et seulement si q”
  - Une condition nécessaire quand p est q ;
  - Une condition suffisante pour q est p.

1.3 Tables de vérité

Les tables de vérité se composent de :
- lignes qui représentent chaque possibilité de combinaison de valeurs pour les propositions atomiques ;
- colonnes qui représentent la valeur de vérité de chaque proposition atomique, puis la valeur de la proposition composée.

p	q	p$\leftrightarrow$q
T	T	T
T	F	F
F	T	F
F	F	T

Table 1 – Table de vérité de la biconditionnelle

Propositions équivalentes

Définition 2. Deux propositions sont équivalentes si elles ont toujours la même valeur de vérité.

2 Équivalences logiques

2.1 Tautologies, contradictions & contingences

Définition 3. Une tautologie est une proposition qui est toujours vraie.

Définition 4. Une contradiction est une proposition qui est toujours fausse.

Définition 5. Une contingence est une proposition qui n'est ni une tautologie ni une contradiction.

2.2 Équivalence logique

Définition 6. Deux propositions sont logiquement équivalentes si p$\leftrightarrow$q est une tautologie. Cela se note p$\Longleftrightarrow$q ou p$\equiv$q.

Lois de *De Morgan*

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

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

Ces propositions sont facilement vérifiables en utilisant des tables de vérité.

Équivalences logiques clés

— Lois d'identité : $p \wedge T = p,\ \ p \vee F = p$;
— Lois de domination : $p \vee T = T, \quad p \wedge F = F$;
— Lois d'impotence : $p \vee p = p,\ \ p \wedge p = p$;
— Loi de double négation : $\neg(\neg p) \equiv p$;
— Lois de négation : $p \vee \neg p \equiv T,\ \ p \wedge \neg p \equiv F$;
— Lois commutatives : $p \vee q \equiv q \vee p,\ \ p \wedge q \equiv q \equiv p$;
— Lois associatives : $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r), \quad (p \vee q) \vee r \equiv p \vee (q \vee r)$;
— Lois distributives : $(p \vee (q \wedge r)) \equiv (p \vee q) \wedge (p \vee r), \quad (p \wedge (q \vee r)) \equiv (p \wedge q) \vee (p \wedge r)$;
— Lois d'absorption : $p \vee (p \wedge q) \equiv p, \quad p \wedge (p \vee q) \equiv p$;

Des équivalences moins fréquentes se trouvent au slide 48. Des preuves d'équivalence y sont aussi décrites.

2.3 Satisfaisabilité compositionnelle

Théorème 7. *Une proposition composée est satisfaisable si il existe une assignation de valeurs de vérité à ses variables telles que la proposition est vraie. Dans le cas contraire, on parle de proposition non-satisfaisable.*

Notation. On écrit $\bigvee_{j=1}^{n}$pour signifier $p_1 \vee p_2 \vee ... \vee p_n$ et $\bigwedge_{j=1}^{n}$pour signifier $p_1 \wedge p_2 \wedge ... \wedge p_n$.

3 Prédicats et quantificateurs

3.1 Prédicats

La logique des prédicats introduit des nouvelles caractéristiques :
- les variables : x, y, z ;
- les prédicats : P(x), M(x) ;
- les quantificateurs :
  - universel : $\forall$;
  - existentiel : $\exists$.

Les fonctions propositionnelles sont une généralisation des propositions. Elles contiennent des variables et des prédicats. Ces variables peuvent être remplacées par des éléments de leur domaine.

Elles deviennent des propositions lorsque leurs variables sont remplacées par des valeurs, ou liées par un quantificateur.

Exemple. P(x) signifie "$x > 0$". Le domaine de x est constitué des entiers. Alors,

- P(-3) est faux ;
- P(0) est faux ;
- P(3) est vrai.

Notation. On note le domaine d'un variable par U.

On peut composer des propositions basée sur des prédicats.

Exemple. Si P(x) signifie "$x > 0$", alors la proposition $P(3) \vee P(-1)$ est vraie.

3.2 Quantificateurs

Les deux quantificateurs les plus importants sont le quantificateur universel ($\forall$) et le quantificateur existentiel ($\exists$). Ceux-ci ont une priorité plus haute que toutes les autres opérateurs logiques.

Notation. $\forall x\, P(x)$ signifie que $P(x)$ est vrai pour tout x dans le domaine. $\exists x\, P(x)$ signifie que $P(x)$ est vrai pour certains x dans le domaine.

On dit que les quantificateurs lient la variable x dans ces expressions.

Un troisième quantificateur signifie que $P(x)$ n'est vrai que pour un et un seul x dans le domaine. Il s'agit de $\exists! x\, P(x)$.

3.3 Équivalence en logique des prédicats

Théorème 8. *Deux déclarations impliquant des prédicats et des quantificateurs sont logiquement équivalentes si elles ont la même valeur de vérité pour chaque prédicat substitué dans ces déclarations, et pour chaque domaine utilisé pour les variables.*

Si le domaine est fini, une proposition universellement quantifiée est équivalente à une conjonction de propositions sans quantificateur, et une proposition existentiellement quantifiée est équivalente à une disjonction de propositions sans quantificateur.

Exemple. Si U = $\{1, 2, 3\}$, alors

$$\forall x\, P(x) \equiv P(1) \wedge P(2) \wedge P(3) \equiv \bigwedge_{x \in U} P(x)$$

$$\exists x\, P(x) \equiv P(1) \vee P(2) \vee P(3) \equiv \bigvee_{x \in U} P(x)$$

3.4 Négation d'expressions quantifiées / lois de *De Morgan*

$$\neg \forall x\, P(x) \equiv \exists x\, \neg P(x)$$

$$\neg \exists x\, P(x) \equiv \forall x\, \neg P(x)$$

4 Quantificateurs imbriqués

4.1 Introduction

Exemple. "Tout nombre a un inverse" s'exprime à l'aide de quantificateurs imbriqués. On écrira $\forall x\, \exists y\, (x + y = 0)$.

4.2 Ordre des quantificateurs

Si l'on assume que $P(x)$ décrit "$x + y = y + x$" et que $\mathbb{U} = \mathbb{Z}$, alors $\forall x\, \forall y\, P(x, y) \equiv \forall y\, \forall x\, P(x, y)$.

Si l'on assume que $Q(x)$ décrit "$x + y = 0$" et que $U = \mathbb{Z}$, alors $\forall x\, \exists y\, P(x, y)$ est vrai, alors que $\exists y\, \forall x\, P(x, y)$ est faux.

4.3 Quantifications de deux variables

Déclaration	Vrai quand ...	Faux quand ...
$\forall x\, \forall y\, P(x, y)$ $\quad$ $\forall y\, \forall x\, P(x, y)$	$P(x, y)$ est vrai pour chaque paire x, y	Il existe une paire telle que $P(x, y)$ est faux
$\forall x\, \exists y\, P(x, y)$	Pour chaque x, il existe un y tel que $P(x, y)$ est vrai	Il existe un x tel que $P(x, y)$ est faux pour chaque y
$\exists x\, \forall y\, P(x, y)$	Il existe un x tel que $P(x, y)$ est vrai pour chaque y	Pour chaque x, il existe un y tel que $P(x, y)$ est faux
$\exists x\, \exists y\, P(x, y)$ $\quad$ $\exists y\, \exists x\, P(x, y)$	Il existe une paire x, y telle que $P(x, y)$ est vrai	$P(x, y)$ est faux pour chaque paire x,y

TABLE 2 – Quantifications de deux variables

5 Règles d'inférence

Un argument est divisé en deux parties : les prémisses qui se placent au-dessus de la ligne, et la conclusion qui se place en-dessous.

$$\frac{\begin{array}{c}\forall x(Homme(x) \rightarrow Mortel(x)) \\ Homme(Socrate)\end{array}}{\therefore Mortel(Socrate)}$$

5.1 Règles concernant la logique propositionnelle

Modus Ponens

$$\frac{\begin{array}{c}p \rightarrow q \\ p\end{array}}{\therefore q}$$

Cet argument est équivalent à la tautologie $(p \wedge (p \rightarrow q)) \rightarrow q$.

Modus Tollens

$$\frac{\begin{array}{c}p \rightarrow q \\ \neg q\end{array}}{\therefore \neg p}$$

Cet argument correspond à la tautologie $(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$.

Syllogisme hypothétique

$$\frac{\begin{array}{c}p \rightarrow q \\ q \rightarrow r\end{array}}{\therefore p \rightarrow r}$$

Cet argument correspond à la tautologie $((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$.

Syllogisme disjonctif

$$\frac{\begin{array}{c}p \vee q \\ \neg p\end{array}}{\therefore q}$$

Cet argument correspond à la tautologie $(\neg p \wedge (p \vee q)) \rightarrow q$.

Addition

$$\frac{p}{\therefore p \lor q}$$

Cet argument correspond à la tautologie $p \rightarrow (p \lor q)$.

Simplification

$$\frac{p \land q}{\therefore q}$$

Cet argument correspond à la tautologie $(p \land q) \rightarrow q$.

Conjonction

$$\begin{array}{c} p \\ q \\ \hline \therefore p \land q \end{array}$$

Cet argument correspond à la tautologie $((p) \land (q)) \rightarrow (p \land q)$.

Résolution

$$\begin{array}{c} \neg p \lor r \\ p \lor q \\ \hline \therefore q \lor r \end{array}$$

Cet argument correspond à la tautologie $((\neg p \lor r) \land (p \lor q)) \rightarrow (q \lor r)$.

5.2 Règles concernant la logique quantificative

Instanciation universelle

$$\frac{\forall x P(x)}{\therefore P(c)}$$

Généralisation universelle

$$\frac{P(c), \text{ c étant arbitraire}}{\therefore \forall x P(x)}$$

Instanciation existentielle

$$\frac{\exists x P(x)}{\therefore P(c) \text{ pour un certain c}}$$

Généralisation existentielle

$$\frac{\therefore P(c) \text{ pour un certain c}}{\exists x P(x)}$$

Modus Ponens universel

$$\frac{\begin{array}{c}\forall x(P(x) \rightarrow Q(x)) \\ P(a), \text{ a étant un élément particulier du domaine}\end{array}}{\therefore Q(a)}$$

6 Formes Normales

6.1 Forme normale disjonctive

Définition 9. Une proposition est dans sa forme normale disjonctive si elle consiste en (1...n) disjonctions où chaque disjonction est une conjonction de (1...m) formules atomiques ou de négations de formules atomiques

Exemple. $(\neg p \wedge q) \vee (p \wedge \neg q)$

6.2 Forme normale conjonctive

Définition 10. Une proposition est dans sa forme normale conjonctive si c'est une conjonction de disjonctions.

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

Toutes les propositions peuvent être réécrites sous leurs formes normales conjonctive et disjonctive.

6.3 Forme normale disjonctive principale

Définition 11. Les mintermes de p et q sont des conjonctions où les variables apparaissent soit niées soit non-niées, mais n'apparaissent pas et niées et non-niées. Les quatre mintermes de p et q sont $p \wedge q$, $p \wedge \neg q$, $\neg p \wedge q$ et $\neg p \wedge \neg q$.

Définition 12. La forme normale disjonctive principale d'une formule est une formule équivalent constituée uniquement de disjonctions de mintermes.

Pour construire une forme normale disjonctive principale, il est nécessaire de remplacer les implications et les équivalences au moyen des opérateurs $\wedge$,$\vee$,$\neg$.

6.4 Forme normale conjonctive principale

Définition 13. Les maxtermes de p et q sont des disjonction où les variables apparaissent soit niées soit non-niées, mais n'apparaissent pas et niées et non-niées. Les quatre maxtermes de p et q sont $p \vee q$, $p \vee \neg q$, $\neg p \vee q$ et $\neg p \vee \neg q$.

Définition 14. La forme normale conjonctive principale d'une formule est une formule équivalente constituée uniquement de conjonctions de maxtermes.

6.5 Forme normale prénexe

Définition 15. Une formule F en logique de premier ordre est dite dans sa forme normale prénexe si et seulement si la formule F est sous forme $(Q_1 x_1)...(Q_n x_n)(M)$ où chaque $Q_i x_i$ est soit $\forall x_i$ soit $\exists x_i$ et M est une formule ne contenant aucun quantificateur. $(Q_1 x_1)...(Q_n x_n)$ est appelé le préfixe et M la matrice de la formule.

Exemple. $(\forall x)(\forall y)(P(x,y) \wedge Q(y))$ est sous forme normale prénexe.

7 Introduction aux preuves

7.1 Preuve directe

Les théorèmes sont souvent sous la forme $\forall x(P(x) \to Q(x))$. On peut les prouver en montrant qu'en prenant un c arbitraire, $P(c) \to Q(c)$ et en utilisant la généralisation universelle.

On assume que p est vrai. On utilise les règles d'inférences, les axiomes et les équivalences logiques afin de montrer que q est obligatoirement vrai.

Exemple. Une preuve directe pour "si n est un entier impair, alors n^2 est impair". On assume que n est impair, donc $n = 2k+1$, $k \in \mathbb{Z}$. Si l'on met les deux cotés de l'équation au carré, on obtient

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

où $r = 2k^2 + 2k$. On a donc montré que si n est un entier impair, alors n^2 est un entier impair.

7.2 Preuve par contraposition

On assume $\neg q$ et on montre que $\neg p$ est aussi vrai. Si l'on donne une preuve que $\neg q \to \neg p$ est vrai, alors on donne aussi une preuve pour $p \to q$.

Exemple. Prouver que si n est un entier et que $3n+2$ est impair, alors n est impair. On assume que n est pair.

$$3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k+1) = 2j$$

pour $j = 3k = 1$. On peut donc dire que $3n+2$ est pair. On a donc prouvé$\neg q \to \neg p$, et donc $p \to q$.

7.3 Preuve par contradiction

Pour prouver p, on assume $\neg p$ et on dérive une contradiction telle que $p \wedge \neg p$. On montre donc que si $\neg p \rightarrow F$ est vrai, alors la contraposée $T \rightarrow p$ est vraie aussi.

Prouver que si l'on choisit 22 jours dans un calendrier, au moins 4 d'entre eux tombent le même jour de la semaine. On commence par assumer que pas plus de 3 des 22 jours tombent le même jour. Comme une semaine contient 7 jours, on n'aurait sélectionné seulement 21 jours. Cela contredit donc le fait que l'on ait choisi 22 jours.

Deuxième partie

Induction et récursion

1 Preuve par induction

Beaucoup de théorèmes déclarent que $P(n)$ est vrai pour tous les entiers positifs, où $P(n)$ est une fonction propositionnelle. L'induction mathématique sert à prouver les théorèmes semblables. Elle se découpe en deux étapes :

— L'étape basique : la proposition $P(1)$ est prouvée vraie ;

— L'étape inductive : l'implication $P(n) \to P(n+1)$ est montrée vraie pour tous les entiers positifs.

$P(n)$ est appelée l'hypothèse inductive.

Exemple. Disons que $P(n)$ dit que la somme des n premiers entiers positifs impairs est n^2.

— Etape basique : $P(1)$: 1 est bien égal à 1^2.

— Etape inductive : On suppose que $P(n)$ est vrai, et donc

$$1 + 3 + 5 + ... + (2n - 1) = n^2.$$

Pour $n + 1$,

$$\begin{aligned} 1 + 3 + 5 + ... + (2n - 1) + (2n + 1) &= [1 + 3 + ... + (2n - 1)] + (2n + 1) \\ &= n^2 + 2n + 1 \\ &= (n + 1)^2. \end{aligned}$$

$P(n+1)$ découle donc bien de $P(n)$. Comme $P(1)$ est vrai et que $P(n) \to P(n+1)$ est vrai pour tous les entiers positifs, $P(n)$ est vrai pour tous les entiers positifs.

Troisième partie

Dénombrement

1 Les bases du dénombrement

1.1 Règle du produit

Théorème 16. *Une procédure peut être décomposée en une séquence de deux tâches. Il existe n_1 façons d'exécuter la première et n_2 façons d'exécuter la deuxième. Il y a alors $n_1.n_2$ façons d'exécuter la procédure.*

Exemple. On a une séquence de 7 bits. Il existe 2^7 séquences différentes possibles.

Notation. $|S|$ représente la taille de l'ensemble S.

Définition 17. Soit S un ensemble. Si S admet exactement n éléments, où n est un entier non négatif, on dit que S est un ensemble fini et que n est la cardinalité de S. On la note $|S|$.

De la règle du produit découlent certaines propriétés :

1. Si A_1, A_2, ... , A_n sont des ensembles finis, alors le nombre d'éléments du produit cartésiens de ces ensembles et le produit du nombre d'éléments de chaque ensemble.
2. Choisir un élément dans le produit cartésien $A_1 \times A_2 \times ... \times A_n$ revient à choisir un élément dans chaque ensemble.
3. La cardinalité du produit cartésien d'ensembles est égale au produit des cardinalités de ces ensemble. $|A_1 \times A_2 \times ... \times A_n| = |A_1|.|A_2|. ... .|A_n|$.

1.2 Règle de la somme

Théorème 18. *Une procédure peut être exécutée de une de n_1 façons, ou de une de n_2 façons, et aucune façon de n_1 n'est égale à une façon de n_2. Il y a alors $n_1 + n_2$ façons d'exécuter la procédure.*

Si l'on parle en terme d'ensembles, $|A \cup B| = |A| + |B|$. En généralisant, cela donne $|A_1 \cup A_2 \cup ... \cup A_n| = |A_1| + |A_2| + ... + |A_n|$, avec $A_i \cap A_j = \emptyset$ pour tout i, j.

Exemple. Il est possible de combiner les règles de somme et de produit. Dénombrons le nombre de séquences qui se composent soit d'une lettre, soit d'une lettre suivie d'un chiffre. On obtient $26 + 26.10 = 286$.

1.3 Règle de la soustraction

Théorème 19. *Une procédure peut être exécutée de une de n_1 façons, ou de une de n_2 façons. Il y a alors $n_1 + n_2$ façons d'exécuter la procédure, en retirant le nombre de tâches communes à n_1 et n_2.*

On écrit $|A \cup B| = |A| + |B| - |A \cap B|$.

1.4 Règle de la division

Théorème 20. *Une procédure peut être exécutée de* n *façons, et, pour chaque façon* f*, il y a exactement* d *façons qui correspondent à* f*. Il y a alors* $^n/_d$ *façons d'exécuter la procédure.*

En termes d'ensembles, on dit : si l'ensemble fini A est l'union de n sous-ensembles disjoints par paires, chacun avec d éléments, alors $n = \frac{|A|}{d}$.

2 Principe du nid de pigeons

Exemple. Combien de cartes doivent-elles êtres sélectionnées dans un jeu de 52 cartes (et placées sur des tas selon leur couleur) afin de s'assurer d'avoir au moins un tas de 3 cartes de la même couleur ? Selon le principe du nid de pigeons, au moins un des tas contient $\frac{N}{4}$ cartes. Le plus petit N tel que $\frac{N}{4} \geq 3$ est 9. Il faut donc tirer 9 cartes pour en avoir au moins 3 de la même couleur.

3 Permutations et combinaisons

3.1 Permutations

Définition 21. Une permutation d'un ensemble d'objets distincts est un arrangement ordonné de ces objets. Un arrangement ordonné de r éléments d'un ensemble est appelée une *r-permutation.*

Notation. Le nombre de r-permutations d'un ensemble constitué de n éléments se note $P(r, n)$.

Théorème 22. *Si* n *est un entier positif et* r *est un entier avec* $1 \leq r \leq n$*, alors il y a* $P(n, r) = n.(n-1).(n-2)...(n-r+1)$ *r-permutations d'un ensemble avec* n *éléments distincts.*

Remarque. $P(n, 0) = 1$.

Corollaire 23. *Si* n *et* r *sont des entiers avec* $1 \leq r \leq n$*, alors* $P(n, r) = \frac{n!}{(n-r)!}$.

3.2 Combinaisons

Définition 24. Une r-combinaison d'éléments dans un ensemble est une sélection non-ordonnée de r éléments de l'ensemble. Une r-combinaison d'un ensemble est donc un sous-ensemble de taille r de cet ensemble.

Notation. Le nombre de r-combinaisons d'un ensemble se note $C(n, r)$. On peut aussi le noter $\binom{n}{r}$, appelé coefficient binomial.

Théorème 25. *Le nombre de r-combinaisons d'un ensemble avec* n *éléments, où* $0 \leq r \leq n$*, est égal à* $C(n, r) = \frac{n!}{(n-r)!r!}$.

Corollaire 26. *Si* r *et* n *sont deux entiers non-négatifs avec* $r \leq n$*,* $C(n, r) = C(n, n-r)$.

3.3 Preuves combinatoires

Définition 27. Une preuve combinatoire d'une identité qui est une preuve qui utilise une des deux méthodes suivantes.

1. Une preuve par double dénombrement utilise des arguments de dénombrement pour prouver que les deux éléments d'une identité comptent le même nombre d'éléments, mais de façon différente.
2. Une preuve bijective démontre qu'il y a une bijection entre les ensembles d'objets comptés par les deux membres de l'identité.

Deux exemples se trouvent sur la slide 40.

4 Coefficients binomiaux et identités

Définition 28. Une expression binomiale est une expression de la somme de deux termes, comme $x + y$.

Théorème 29. *Identité de Pascal. n et k sont deux entiers positifs avec $n \geq k$. Alors,*

$$C(n+1,k) = C(n,k-1) + C(n,k)$$

Théorème 30. *Théorème binomial. Soient x et y, deux variables, et n un entier non-négatif. Alors,*

$$\begin{aligned} (x+y)^n &= \sum_{j=0}^{n} C(n,j)x^{n-j}y^j \\ &= C(n,0)x^n + C(n,1)x^{n-1}y + ... + C(n,n-1)xy^{n-1} + C(n,n)y^n \end{aligned}$$

Corollaire 31. *Avec $n \geq 0$,*

$$\sum_{k=0}^{n} C(n,k) = 2^n$$

5 Permutations et combinaisons généralisées

5.1 Permutations avec répétition

Théorème 32. *Le nombre de r-permutations d'un ensemble de n objets avec répétition autorisée vaut n^r.*

5.2 Combinaisons avec répétition

Théorème 33. *Le nombre de r-combinaisons d'un ensemble de n objets avec répétition autorisée vaut $C(n+r-1,r) = C(n+r-1,n-1)$.*

5.3 Permutations avec des objets indistinguables

Théorème 34. *Le nombre de permutations différentes de n objets, où il y a n_1 objets indistinguables de type 1, n_2 objets indistinguables de type 2, ... , $n_k$objets indistinguables de type k, est*

$$\frac{n!}{n_1!n_2!...n_3!}$$

Quatrième partie

Techniques de dénombrement avancées

1 Applications des relations de récurrence

Définition 35. Une relation de récurrence pour la séquence $\{a_n\}$ est une équation qui exprime a_n en termes d'un ou plus des termes précédents de la séquence, i.e., $a_0, a_{1,}, ..., a_{n-1}$ avec n un entier non-négatif $\geq n_0$.

Définition 36. Une séquence est appelée solution d'une relation de récurrence si ses termes satisfont la relation.

Définition 37. Les conditions initiales d'une séquence spécifient les termes qui précèdent le premier terme où la relation de récurrence prend effet.

2 Résolution des relations de récurrence linéaires

2.1 Relations de récurrence linéaires homogènes

Définition 38. Une relation de récurrence linéaire homogène de degré k à coefficients constants est une équation de récurrence du type $a_n = c_1a_{n-1} + c_2a_{n-2} + ... + c_ka_{n-k}$, où $c_1, c_2, ..., c_k$ sont des nombres réels et $c_k \neq 0$.

Elle est linéaire car la partie droite de l'équation est une somme des termes précédents de la séquence, chacun étant multiplié par une fonction de n.

Elle est homogène car il n'y a pas de termes qui ne sont pas des multiples de a. Son degré est k car elle est exprimée en fonction des k termes précédents de la séquence.

Exemple. $f_n = f_{n-1} + f_{n-2}$ est une relation de récurrence linéaire homogène de degré 2.

1. On regarde pour des solutions du type $a_n = r^n$, où r est constant.
2. On écrit l'équation caractéristique grâce à des manipulations algébriques.

$$r^k - c_1r^{k-1} - ... - c_{k-1}r - c_k$$

3. La séquence $\{a_n\}$ avec $a_n = r^n$ est solution si et seulement si r^n est solution de l'équation caractéristique.
4. Les solutions de l'équation caractéristique sont appelées les racines caractéristiques de la relation de récurrence. Elles sont utilisées pour donner une formule explicite pour toutes les solutions de la relation de récurrence.

Relations de degré 2

Théorème 39. *Soient c_1 et c_2 des nombres réels. Supposons que $r^2 - c_1 r - c_2 = 0$ a deux racines, r_1 et r_2. Alors, la séquence $\{a_n\}$ est une solution de la relation de récurrence $a_n = c_1 a_{n-1} + c_2 a_{n-2}$ si et seulement si $a_n = \alpha_1 r_1^n + \alpha_2 r_2^n$ pour $n = 0, 1, 2, ...$ et pour α_1 et α_2 constants.*

Exemple. Trouvons la solution de la relation de récurrence $a_n = a_{n-1} + 2a_{n-2}$ avec $a_0 = 2, a_1 = 7$.

1. L'équation caractéristique est $r^2 - r - 2 = 0$. Ses racines sont 2 et -1.
2. $\{a_n\}$ est donc solution de la relation si et seulement si $a_n = \alpha_1 2^n + \alpha_2 (-1)^n$.
3. Grâce aux conditions initiales, on trouve que $a_0 = 2 = \alpha_1 + \alpha_2$ et $a_1 = 7 = 2\alpha_1 - \alpha_2$. En résolvant le système, on obtient $\alpha_1 = 3, \alpha_2 = -1$.
4. La solution est donc $\{a_n\}$ avec $a_n = 3.2^n - (-1)^n$.

Avec une racine répétée

Théorème 40. *Soient c_1 et $c_2 \neq 0$ des nombres réels. Supposons que $r^2 - c_1 r - c_2 = 0$ a un racine répétée, r_0. Alors, la séquence $\{a_n\}$ est une solution de la relation de récurrence $a_n = c_1 a_{n-1} + c_2 a_{n-2}$ si et seulement si $a_n = \alpha_1 r_0^n + \alpha_2 n r_0^n$ pour $n = 0, 1, 2, ...$ et pour α_1 et α_2 constants.*

Relations de degré k

Théorème 41. *Soient c_1,c_2,...,c_k des nombres réels. Supposons que $r^k - c_1 r^{k-1} - ... - c_k = 0$ a k racines, r_1,r_2,...,r_k. Alors, la séquence $\{a_n\}$ est une solution de la relation de récurrence $a_n = c_1 a_{n-1} + c_2 a_{n-2} + ... + c_k a_{n-k}$ si et seulement si $a_n = \alpha_1 r_1^n + \alpha_2 r_2^n + ... + \alpha_k r_k^n$ pour $n = 0, 1, 2, ...$ et pour α_1,α_2,...,α_k constants.*

Cas général pour les racines répétées

Théorème 42. *Soient c_1, c_2, ... , c_k des nombres réels et l'équation caractéristique*

$$r^k - c_1 r^{k-1} - ... - c_k$$

qui a t racines distinctes r_1, r_2, ... , r_t avec des multiplicités (c'est-à-dire le nombre de fois que la racine est présente) m_1, m_2, ... , m_t, telles quel $m_i \geq 0, 1, 2, ...$ et que $m_1 + m_2 + ... + m_t = k$. Alors, la séquence $\{a_n\}$ est une solution de la relation de récurrence

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + ... + c_k a_{n-k}$$

si et seulement si

$$\begin{aligned} a_n &= (\alpha_{1,0} + \alpha_{1,1} n + ... + \alpha_{1,m_1-1} n^{m_1-1})\, r_1^n \\ &+ (\alpha_{2,0} + \alpha_{2,1} n + ... + \alpha_{2,m_2-1} n^{m_2-1})\, r_2^n \\ &\vdots \\ &+ (\alpha_{t,0} + \alpha_{t,1} n + ... + \alpha_{t,m_t-1} n^{m_t-1})\, r_t^n \end{aligned}$$

pour $n = 0$, 1, 2, ... où $\alpha_{i,j}$ sont des constantes pour $1 \leq i \leq t$ et $0 \leq j \leq m_i - 1$.

2.2 Relations de récurrence linéaires non-homogènes

Définition 43. Une relation de récurrence linéaire non-homogène de degré k à coefficients constants est une équation de récurrence du type $a_n = c_1 a_{n-1} + c_2 a_{n-2} + ... + c_k a_{n-k} + F(n)$, où $c_1, c_2, ..., c_k$ sont des nombres réels et $c_k \neq 0$ et $F(n)$ est une fonction non nulle dépendant seulement de n.

La relation $a_n = c_1 a_{n-1} + c_2 a_{n-2} + ... + c_k a_{n-k}$ est appelée la relation de récurrence homogène associée.

Théorème 44. *Si $\left\{a_n^{(p)}\right\}$ est une solution particulière de la relation $a_n = c_1 a_{n-1} + c_2 a_{n-2} + ... + c_k a_{n-k} + F(n)$, alors toutes les solutions sont de la forme $\{a_n^{(p)} + a_n^{(h)}\}$ où $\left\{a_n^{(h)}\right\}$ est une solution de la relation homogène associée.*

3 Inclusion-Exclusion

Cas de 3 ensembles finis

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

4 Approche état-espace

Soit l'équation de récurrence

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + ... + c_k a_{n-k} + F(n)$$

et mettons-là sous forme de vecteurs / matrices :

$$a_n = \begin{bmatrix} a_n \\ a_{n-1} \\ \vdots \\ a_{n-k+1} \end{bmatrix} \qquad a_{n-1} = \begin{bmatrix} a_{n-1} \\ a_{n-2} \\ \vdots \\ a_{n-k} \end{bmatrix} \qquad f_n = \begin{bmatrix} F(n) \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

Définissons la matrice

$$C = \begin{pmatrix} c_1 & c_2 & c_3 & \cdots & c_{k-1} & c_k \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$$

On obtient donc une équation $a_n = Ca_{n-i} + f_n$. En sachant que a_0 est donné, on peut résoudre l'équation

$$\begin{cases} a_1 & = Ca_0 + f_1 \\ a_2 & = Ca_1 + f_2 = C^2 a_0 + Cf_1 + f_2 \\ a_3 & = Ca_2 + f_3 = C^3 a_0 + C^2 f_1 + Cf_2 + f_3 \\ \vdots \end{cases}$$

On peut donc inférer que

$$a_n = C^n a_0 + \sum_{k=1}^{n} C^{k-1} f_{n-k+1}$$

Cinquième partie

Graphes

1 Graphes et modèles de graphes

Définition 45. Un graphe $G = (V, E)$ consiste en un ensemble non-vide V de nœuds et un ensemble E d'arcs. Chaque arc a soit un soit deux nœuds associés à elle-même, appelés ses extrémités. On dit qu'un arc connecte ses extrémités.

Dans un graphe simple, chaque arc connecte deux nœuds différents et il n'y pas deux arcs entre deux noeuds.

Dans un multigraphe, il peut y avoir plusieurs (m) arcs entre deux nœuds u et v. On dit alors que {u, v} est un arc de multiplicité m.

Un pseudographe est un multigraphe auquel on ajoute le concept de boucle.

Définition 46. Un graphe dirigé $G = (V, E)$ consiste en un ensemble non-vide V de nœuds et un ensemble E d'arcs dirigés. L'arc associé à la paire ordonnée (u,v) démarre de u et finit à v.

Type	Arcs	Arcs multiples ?	Boucles ?
Graphe simple	Non-dirigés	$\times$	$\times$
Multigraphe	Non-dirigés	$\surd$	$\times$
Pseudographe	Non-dirigés	$\surd$	$\surd$
Graphe dirigé simple	Dirigés	$\times$	$\times$
Multigraphe dirigé	Dirigés	$\surd$	$\times$
Graphe mixte	Dirigés & non-dirigés	$\surd$	$\surd$

TABLE 3 – Types de graphes et propriétés

2 Terminologie et types de graphes spéciaux

2.1 Terminologie basique

Définition 47. Deux noeuds u, v d'un graphe non-dirigé G sont adjacents, ou voisins, dans G s'il y a un arc e entre u et v. Cet arc est incident avec les arcs u et v.

Définition 48. L'ensemble de tous les voisins d'un noeud v de G, noté $N(v)$, s'appelle le voisinage de v. Si A est un sous-ensemble de V, on note $N(A)$ l'ensemble de tous les noeuds de G voisins d'au moins un des noeuds de A.

Définition 49. Le degré d'un noeud d'un graphe non-dirigé est les nombre d'arcs incidents avec lui. Une boucle compte double. Le degré du noeud v se note $deg(v)$.

Théorème 50. *Si $G = (V, E)$ est un graphe non-dirigé avec m arcs, alors*

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

Théorème 51. *Un graphe non-dirigé a un nombre pair de noeuds de degré impair.*

Définition 52. Le degré entrant de v, noté $deg^{-}(v)$, est le nombre d'arcs qui finissent à v. Le degré sortant de v, noté $deg^{+}(v)$, est le nombre d'arcs dont v est le noeud initial. Une boucle compte pour 1 et dans le degré entrant et dans le degré sortant.

Théorème 53. *Soit $G = (V, E)$ un graphe avec des arcs dirigés. Alors,*

$$|E| = \sum_{v \in V} deg^{-}(v) + \sum_{v \in V} deg^{+}(v)$$

2.2 Types spéciaux de graphes simples

Graphes complets

Définition 54. Un graphe complet sur n noeuds, noté K_n, est le graphe simple qui contient exactement un arc entre chaque paire de noeuds distincts.

Cycles et roues

Définition 55. Un cycle C_n pour $n \geq 3$ consiste en n noeuds $v_1, v_2, ..., v_n$ et en les arcs $\{v_1, v_2\}$, $\{v_2, v_3\}$, ... , $\{v_{n-1}, v_n\}$.

Définition 56. Une roue est un cycle auquel on a rajouté un noeud. Ce noeud est relié à tous les autres noeuds.

2.3 Graphes bipartis

Définition 57. Un simple graphe est biparti si V peut être partitionné en deux sous-ensembles distincts, V_1et V_2, de façon à ce que chaque arc relie un noeud dans V_1 et un noeud dans V_2.

Définition 58. Un graphe biparti complet $K_{m,n}$ est un graphe qui a ses noeuds séparés en en deux sous-ensembles V_1 de taille m et V_2 de taille n, de telle sorte qu'il y ait un arc de chaque noeud de V_1 vers chaque noeud de V_2.

2.4 Graphes construits à partir d'autres

Définition 59. Un sous-graphe d'un graphe $G = (V, E)$ est un graphe (W, F) où $W \subset V$ et $F \subset E$. Un sous-graphe H de G est un sous-graphe propre si $H \neq G$.

Définition 60. Soit $G = (V, E)$ un graphe simple. Le sous-graphe induit par un sous-ensemble W de V est le graphe (W, F), où l'ensemble des arcs F ne contient un arc dans E que si les deux extrémités se trouvent dans W.

Définition 61. L'union de deux graphes simples $G_1 = (V_1, E_1)$ et $G_2 = (V_2, E_2)$ est le graphe simple avec comme ensemble de noeuds $V_1 \cup V_2$ et comme ensemble d'arcs $E_1 \cup E_2$. L'union des deux graphes s'écrit $G_1 \cup G_2$.

3 Représentation et isomorphisme de graphes

3.1 Liste d'adjacence

Définition 62. Une liste d'adjacence peut être utilisée pour représenter un graphe sans arcs multiples en spécifiant quels noeuds sont adjacents à chaque noeud du graphe.

3.2 Matrice d'adjacence

Définition 63. Soit $G = (V, E)$ un graphe simple où $|V| = n$. La matrice d'adjacence A_G de G est la matrice binaire $n \times n$ où, si

— v_i et v_j sont adjacents, alors $a_{ij} = 1$;
— v_i et v_j ne sont sont pas adjacents, alors $a_{ij} = 0$.

Une matrice d'adjacence peut aussi être utilisée pour représenter des multigraphes par exemple. Elle ne sera alors plus binaire, et a_{ij} représentera le nombre d'arcs entre les noeuds i et j. Dans le cas de graphes dirigés, la matrice ne sera plus symétrique.

3.3 Matrice d'incidence

Définition 64. Soit $G = (V, E)$ un graphe non-dirigé avec n noeuds et m arcs. La matrice d'incidence est la matrice $n \times m$ M où $m_{ij} = 1$ si l'arc e_j est incident avec v_i, et 0 sinon.

3.4 Graphes isomorphes

Définition 65. Les graphes simples $G_1 = (V_1, E_1)$ et $G_2 = (V_2, E_2)$ sont isomorphes s'il y a une bijection f de V_1 à V_2 avec la propriété que a et b sont adjacents dans G_1 si et seulement si $f(a)$ et$f(b)$ sont adjacents dans G_2, pour tout a, b dans V_1.

4 Connexité

4.1 Chemins

Définition 66. Un chemin est une séquence d'arcs qui commence au noeud d'un graphe et qui voyage de noeud en noeud en suivant les arcs du graphe.

Définition 67. Soit n un entier non-négatif et G un graphe non-dirigé. Un chemin de longueur n de u à v dans G est une séquence de n arcs de G pour lesquels il existe une séquence $x_0 = u, x_1, ..., x_{n-1}$, $x_n = v$ de noeuds telle que e_i a pour $i = 1, ..., n$, les extrémités x_{i-1} et x_i.

Quand le graphe est simple, on peut décrire ce chemin simplement en citant les noeuds par lesquels il passe.

Le chemin est un circuit si $u = v$ et qu'il a une longueur non-nulle.

Un chemin est simple s'il ne passe pas plus d'une fois par chaque arc.

4.2 Connexité dans un graphe non-dirigé

Définition 68. Un graphe non-dirigé est dit connexe si il y a un chemin entre chaque paire de noeuds.

Définition 69. Une composante connexe d'un graphe est un sous-graphe connexe de G qui n'est pas un sous-graphe propre d'un autre sous-graphe connexe de G.

4.3 Connexité dans un graphe dirigé

Définition 70. Un graphe dirigé est fortement connexe s'il existe un chemin de a vers b et de b vers a quels que soient a et b dans le graphe.

Définition 71. Un graphe dirigé est faiblement connexe s'il existe un chemin entre a et b dans le graphe non-dirigé correspondant.

Définition 72. Les sous-graphes d'un graphe dirigé qui sont fortement connexes mais qui ne sont pas contenus dans d'autres sous-graphes connexes plus larges (le sous-graphe fortement connexe maximal) sont appelés les composantes fortement connexes de G.

4.4 Dénombrer les chemins entre deux noeuds

Théorème 73. *Soit G un graphe et A sa matrice d'adjacence. Le nombre de chemins différents de longueur r de v_i à v_j, où $r > 0$, est égal à la $(i, j)^e$ position de A^r.*

5 Chemins d'Euler et de Hamilton

5.1 Chemins et circuits d'Euler

Définition 74. Un circuit d'Euler dans un graphe G est un circuit simple qui contient tous les arcs de G.

Définition 75. Un chemin d'Euler est un chemin simple qui contient tous les arcs du graphe.

Théorème 76. *Un multigraphe connexe avec au moins deux noeuds a un circuit d'Euler si et seulement si chacun de ses noeuds a un degré pair. Il a un circuit d'Euler si et seulement si exactement deux noeuds du graphe ont un degré impair.*

Conditions nécessaires pour les circuits et les chemins d'Euler

- Le circuit d'Euler commence au noeud a et continue avec un arc reliant a à b. L'arc contribue à hauteur de 1 dans $deg(a)$.
- Chaque fois que le circuit passe par un noeud, il contribue à hauteur de 2 dans le degré du noeud.
- Le circuit se termine à a, et contribue a hauteur de 1 à $deg(a)$. Celui-ci est donc pair.
- Tous les autres degrés sont pairs.
- Si ce n'est pas un circuit mais un chemin, les noeuds initial et final ont un degré impair.

Algorithme pour construire un circuit d'Euler

Algorithme 1 Construction d'un circuit d'Euler

```
procedure Euler(G : multigraphe connexe dont tous les noeuds ont un degré pair)

    circuit := un circuit dans G commençant à un noeud arbitraire, avec des arcs
        ajoutés successivement pour former un chemin qui retourne au noeud initial
    H := G avec les arcs du circuit retirés

    while H a des arcs
        subcircuit := un circuit avec H commençant a un noeud de H qui est aussi une
            des extrémités d un arc du circuit principal
        H := H dont on retire les arcs de subcircuit et tous les noeuds isolés
        circuit := circuit où l on insère subcircuit au noeud approprié

return circuit
```

5.2 Chemins et circuits d'Hamilton

Les chemins et circuits d'Hamilton se basent sur le même principe que ceux d'Euler, à la différence près qu'on ne cherche plus à ne passer par chaque arc qu'une fois mais bien à ce que chaque noeud ne soit traversé qu'une et une seule fois.

Définition 77. Un chemin simple dans un graphe G qui passe par chaque noeud exactement une fois est appelé chemin d'Hamilton. Il en va de même pour les circuits.

6 Problèmes du chemin minimal

6.1 Algorithme de Dijkstra

Définition 78. Un graphe qui a un nombre assigné à chaque arc est appelé un graphe pondéré.

Définition 79. Le poids d'un chemin dans un graphe est la somme des poids des arcs qui constituent le chemin.

Théorème 80. *Algorithme de Dijkstra. L'algorithme de Dijkstra calcule la longueur du plus court chemin entre deux noeuds d'un graphe simple pondéré non-dirigé.*

Algorithme 2 Dijkstra

```
procedure Dijkstra(G : graphe simple connexe pondéré)
    {G a des noeuds v, des longueurs w où w(v1,v2) = inf si (v1,v2)
        n est pas un arc dans G, le premier noeud est a, le dernier
        est z}

    for i:=1 to n
        L(v(i)) := inf
    L(a) := 0
    S := vide

    while z n est pas dans S
        u := un noeud pas dans S avec L(u) minimal
        S := S où l on rajoute u
        for tous les noeuds non compris dans S
            if L(u) + w(u,v) < L(v)
                then L(v) := L(u) + w(u,v)

return L(z)
```

Théorème 81. *Tout sous-chemin d'un chemin minimal doit être lui-même un chemin minimal.*

Théorème 82. *Preuve de l'algorithme de Dijkstra. Voir slides 96-100.*

7 Graphes planaires

Définition 83. Un graphe est dit planaire si il peut être dessiné sans qu'aucun de ses arcs ne se croise.

Théorème 84. *Formule d'Euler. Soit G un graphe planaire connexe avec e arcs et v noeuds. Soit r le nombre de régions d'une représentation planaire de G. Alors*

$$r = e - v + 2$$

8 Coloration de graphe

Définition 85. La coloration d'un graphe simple est l'assignation d'une couleur à chaque noeud de façon à ce qu'aucun noeud adjacent n'ait la même couleur. Le nombre minimal de couleurs nécessaires à la coloration d'un graphe est appelé le nombre chromatique du graphe.

Théorème 86. *Le nombre chromatique d'un graphe n'est jamais supérieur à 4. La preuve de ce théorème est très complexe.*

9 L'algorithme PageRank

9.1 Le PageRank basique

1. A chaque page i, on associe un score x_i, proportionnel au score pondéré moyen des pages pointant vers i.
2. Soit w_{ij} le poids du lien connectant la page i à la page j, généralement 1 ou 0 (1 si un lien, 0 si pas).
3. Soit W la matrice contenant les éléments w_{ij}. On assume que le graphe est fortement connexe. On a donc

$$x_i \propto \sum_{j=1}^{n} \frac{w_{ji} x_j}{w_j}$$

   où $w_j = \sum_{i=1}^{n} w_{ji}$, c'est-à-dire le degré sortant de la page j.
4. Si l'on définit la probabilité de suivre le lien de la page j à la page i comme étant

$$P(page(k+1) = i \mid page(k) = j) = \frac{w_{ji}}{w_j}$$

   on peut écrire

$$x_i(k+1) = P(page(k+1) = i) = \sum_{j=1}^{n} P(page(k+1) = i) \,|\, page(k) = j) x_j(k)$$

   C'est-à-dire la somme des probabilités de naviguer sur une page multipliées par la probabilité de transition de celles-ci.
5. Appelons P la matrice des probabilités de transition, avec

$$p_{ij} = P(page(k+1) = j \mid page(k) = i)$$

   On peut réécrire l'équation comme étant

$$x_i(k+1) = \sum_{j=1}^{n} p_{ji} x_j(k)$$

6. Sous la forme de matrice, si le vecteur x a des éléments x_i,

$$x(k+1) = P^T x(k)$$

7. La distribution stationnaire (non-vue au cours) nous dit que $x = P^T x$.

9.2 Ajustements

En autorisant le saut aléatoire sur n'importe quel noeud dans le graphe, cela donne

$$G = \alpha P + (1 - \alpha) \frac{ee^T}{n}$$

où e est un vecteur colonne rempli de 1 et $0 \leq \alpha \leq 1$. Cela permet de ne pas rester coincé dans un noeud absorbant et de traiter les composantes séparées. Plus de détails sont disponibles dans les slides.