Informatique théorique III
(Automates, langages & calculabilité)

Formulaire du Cours 2004-2005
Partie 1
EPFL – I&C

Uwe Nestmann
Sébastien Briais
Daniel C. Bünzli

14 février 2005

Bibliographie

[HMU03] John Hopcroft, Rajeev Motwani, and Jeffrey Ullman. *Introduction to Automata Theory, Languages and Computation*. Pearson Education International, 2003. ISBN 0321210298.

[Koz97] Dexter Kozen. *Automata and Computability*. Springer Verlag New York Inc., 1997.

[Sch01] Carol Schumacher. *Chapter Zero — Fundamental Notions of Abstract Mathematics*. Addison Wesley, 2001.

[Sip97] Michael Sipser. *Introduction to the Theory of Computation*. PWS Publishing Company, 1997.

[Wol01] Pierre Wolper. *Introduction à la calculabilité — Cours et exercices corrigés*. Dunod, Paris, 2001. 2^e édition.

Table des matières

Plan du cours

$Id: notes-prelim.tex,v 1.40 2004/11/22 15:15:40 uwe Exp $

La plupart du matériel est tiré des livres mentionnés dans la bibliographie. Cependant, le livre principal est [HMU03] qui est recommandé à tous les participants du cours.

La répartition planifiée du matériel sur les semaines se trouve sur la page web du cours qui se trouve à

`http://lamp.epfl.ch/teaching/it3/2004/html/`

mais les semaines sont aussi indiqués sur les marges de ce document-ci.

Chapitre 0

Préliminaires

0.1 Notations

Pour clarifier nos propositions mathématiques nous utilisons une notation logique informelle. Pour des propositions quelconques A et B, nous écrivons,

- $A \wedge B$ pour (A et B), la conjonction de A et de B.
- $A \vee B$ pour (A ou B), la disjonction de A et de B.
- $\neg A$ pour (non A), la négation de A.
- $A \Rightarrow B$ pour (A implique B), qui signifie (si A alors B)
- $A \Leftrightarrow B$ pour (A ssi B) qui abrège (A si et seulement si B) et qui exprime l'équivalence logique de A et de B.

Pour nier des relations entre des objets mathématiques, nous tracons le symbole relationnel. Par exemple pour la relation d'égalité nous écrivons $A \neq B$ au lieu $\neg(A = B)$.

Une proposition $P(x, y)$ avec variables x et y est appellée un *prédicat*. Elle devient vraie ou fausse lorsque x et y sont remplacés par des objets particuliers. Pour quantifier les variables nous utilisons,

- $\exists x.\, P(x)$ pour (il existe x tel que $P(x)$), la quantification existentielle d'une variable.
- $\forall x.\, P(x)$ pour (pour tout x tel que $P(x)$), la quantification universelle d'une variable.

Nous utilisons fréquement les abréviations suivantes,

- $\exists x, y, \ldots, z.\, P(x)$ abrège $\exists x \exists y \ldots \exists z.\, P(x)$
- $\forall x, y, \ldots, z.\, P(x)$ abrège $\forall x \forall y \ldots \forall z.\, P(x)$.

Parfois il est pratique de pouvoir spécifier l'ensemble X auquel appartient la variable quantifiée. Nous écrivons donc,

- $\exists x \in X.\, P(x)$ pour $\exists x.\, x \in X \Rightarrow P(x)$
- $\forall x \in X.\, P(x)$ pour $\forall x.\, x \in X \Rightarrow P(x)$.

Finalement, nous écrivons $\exists! x.\, P(x)$, le quantificateur d'unicité qui affirme l'existence *unique* d'un objet x satisfaisant le prédicat $P(x)$. Ce dernier quantificateur n'est que l'abréviation de

$$\big(\exists x.\, P(x)\big) \wedge \big(\forall y, z.\, P(y) \wedge P(z) \Rightarrow y = z\big).$$

Lorsque nous souhaitons nommer par un identificateur A un objet mathématique X nous écrivons,

$$A \triangleq X$$

Cette notation est à distinguer de $A = X$ qui exprime une égalité entre deux objets mathématiques A et B.

0.2 Ensembles

Un ensemble est une collection non ordonnée d'objets dont on dit qu'ils sont les *éléments* ou *membres* de l'ensemble. Par convention les noms d'ensembles sont notés en majuscule. Nous écrivons $a \in A$ l'appartenance de l'objet a à l'ensemble A et $\{a, b, c, \dots\}$ l'ensemble dont les éléments sont a, b, c, ...

Les ensembles suivants, dont on suppose l'existence, sont particulièrement importants.

- $\emptyset$, l'ensemble vide qui ne contient aucun élément. Il est caractérisé par la proposition $\forall x. x \notin \emptyset$.
- $\mathbb{N} \triangleq \{ 0, 1, 2, 3, \dots \}$, l'ensemble des nombres naturels.
- $\mathbb{N}^* \triangleq \mathbb{N} \setminus \{ 0 \}$, l'ensemble des nombre naturels positifs.
- $[n, m] \triangleq \{n \in \mathbb{N} \mid n \leq i \wedge i \leq m\}$, pour $n, m \in \mathbb{N}$.
- $\mathbb{Z} \triangleq \{ \dots, -2, -1, 0, 1, 2, \dots \}$, l'ensemble des nombres entiers (relatifs).

0.2.1 Définition (Sous-ensemble et égalité) A est un *sous-ensemble* de B, noté $A \subseteq B$ ssi tout élément de A est un élément de B,

$$A \subseteq B \Leftrightarrow \forall x \in A. x \in B$$

Deux ensemble A et B sont *égaux*, noté $A = B$, ssi A est inclus dans B et vice-versa,

$$A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A$$

Un ensemble A est un *sous-ensemble strict* de B, noté $A \subset B$ ssi il est sous-ensemble de B mais qu'il n'est pas égal à B.

$$A \subset B \Leftrightarrow A \subseteq B \wedge B \nsubseteq A$$

□

Pour construire des ensembles à partir d'autres ensembles nous utilisons les opérations suivantes.

0.2.2 Définition (Opérations sur les ensembles)

Compréhension. Si X est un ensemble et $P(x)$ un prédicat alors nous pouvons former l'ensemble

$$\{x \in X \mid P(x)\}$$

que l'on écrit aussi parfois $\{x \mid x \in X \wedge P(x)\}$. Il caractérise le plus grand sous-ensemble de X dont les éléments satisfont $P(x)$.

Indexation. Si I est un ensemble et que pour tout $i \in I$ il y a un objet x_i alors on peut former l'ensemble

$$\{x_i \mid i \in I\}$$

dont les éléments x_i sont dits *indexés* par les éléments de I.

Union. L'union $A \cup B$ de deux ensembles A et B contient les éléments de chacun de ceux-ci.

$$A \cup B \triangleq \{x \mid x \in A \vee x \in B\}$$

Intersection. L'intersection $A \cap B$ de deux ensembles A et B contient les éléments présent dans chacun de ceux-ci.

$$A \cap B \triangleq \{x \mid x \in A \wedge x \in B\}$$

Produit. Le produit $A \times B$ de deux ensembles est l'ensemble des paires (x, y) ordonnées dont la première composante est dans A et la seconde dans B.

$$A \times B \triangleq \{(x, y) \mid x \in A \wedge y \in B\}$$

Complément. Le complément $A \backslash B$ d'un ensemble B relativement à un ensemble A, est l'ensemble A dont les éléments de B sont soustraits.

$$A \backslash B \triangleq \{x \mid x \in A \wedge x \notin B\}$$

Lorsque l'ensemble A est implicite ou évident dans le contexte, on écrit simplement $\overline{B}$ pour $A \backslash B$.

Ensemble des parties. L'ensemble des parties $\mathcal{P}(A)$ d'un ensemble A est l'ensemble des sous-ensembles de A.

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

0.3 Relations

Une *relation* n-aire sur une collection d'ensembles $A_1, \ldots, A_n$ est un ensemble $R \subseteq A_1 \times \ldots \times A_n$. Les éléments $x_1 \in A_1, \ldots, x_n \in A_n$ sont dit *reliés* par R si $(x_1, \ldots, x_n) \in R$. Une relation est un ensemble et l'ensemble des relations sur la collection $A_1, \ldots, A_n$ est l'ensemble d'ensembles $\mathcal{P}(A_1 \times \ldots A_n)$.

Une relation unaire P sur un ensemble A est appelée un *prédicat*. On dit que P est vraie pour un élément $x \in A$ ssi $x \in P$. Au lieu de noter $x \in P$ l'on note parfois $P(x)$, en interprétant P comme une fonction qui associe les éléments de A aux valeurs de vérité.

Pour une relation binaire $R \subseteq A \times B$ sur deux ensembles A et B nous écrivons parfois aRb au lieu de $(a, b) \in R$.

0.3.1 Définition (Identité) L'identité id_A sur un ensemble A est la relation binaire sur $A \times A$ définie par $\mathrm{id}_A \triangleq \{(x, x) \mid x \in A\}$. □

0.3.2 Définition (Propriétés des relations binaires) Une relation binaire $R \subseteq A \times A$ sur un ensemble A est,

réflexive si $\forall a \in A.\, aRa$,

irréflexive si $\forall a \in A.\, \neg aRa$,

symétrique si $\forall a, b \in A.\, aRb \Rightarrow bRa$,

antisymétrique si $\forall a, b \in A.\, (aRb \wedge bRa) \Rightarrow a = b$,

transitive si $\forall a, b, c \in A.\, (aRb \wedge bRc) \Rightarrow aRc$,

totale si $\forall a, b \in A.\, aRb \vee bRa$,

une trichotomie si $\forall a, b \in A.\, aRb \vee a = b \vee bRa$ □

Pour construire des relations à partir d'autres relations nous utilisons notamment les opérations suivantes.

0.3.3 Définition (Opérations sur les relations)

Raffinement. Soit R une relation, R' est un raffinement de R si $R' \subseteq R$.

Inverse. Soit $R \subseteq A \times B$ une relation, l'inverse (ou l'opposé) $R^{-1} \subseteq B \times A$ d'une relation R est défini par

$$R^{-1} \triangleq \{(b, a) \in B \times A \mid (a, b) \in R\}$$

Composition. Soit $R \subseteq A \times B$ et $R' \subseteq B \times C$ la composition $RR' \subseteq A \times C$ de R et de R' est définie par,

$$RR' \triangleq \{(a, c) \in A \times C \mid \exists b \in B.(a, b) \in R \wedge (b, c) \in R'\}$$

La composition RR' est aussi notée $R' \circ R$ (notamment pour les fonctions).

Fermeture réflexive. Soit R une relation, la fermeture réflexive est la plus petite relation réflexive R' qui contient R.

Fermeture transitive. Soit R une relation, la fermeture transitive R^+ de R est la plus petite relation transitive qui contient R. La fermeture transitive et réflexive d'une relation R est notée R^*. □

0.3.4 Lemme

1. Si R est symétrique alors $R = R^{-1}$.
2. Soit $R \subset A \times A$, la relation $R' \triangleq R \cup \{(a, a) \mid A \in A\}$ est la fermeture réflexive de R.
3. Soit $R \subset A \times A$, et la suite de relation R^i définie par induction de la manière suivante,

$$R^1 \triangleq R \qquad R^{i+1} \triangleq R\, R^i$$

alors l'ensemble $R^+ \triangleq \bigcup_{i \in \mathbb{N}} R_i$ est la fermeture transitive de R. □

0.3.5 Définition (Ordres) Soit A un ensemble et $R \subseteq A \times A$ une relation.

Pré-ordre. Le couple (A, R) est un pré-ordre si R est réflexive et transitive.

Ordre (partiel). Le pré-ordre (A, R) est un ordre (partiel) si R est antisymétrique.

Ordre total. L'ordre (A, R) est un ordre total si de plus R est totale.

Ordre strict. Le couple (A, R) est un ordre strict si R est irréflexive et transitive.

Ordre total strict. Le couple (A, R) est un ordre total strict si (A, R) est un ordre strict et R est une trichotomie.

En général, on utilise les symboles $\leq$, $\preceq$ et $\sqsubseteq$ pour les ordres, $<$, $\prec$ et $\sqsubset$ pour les ordres stricts. □

0.3.6 Définition (Relation d'équivalence) Une *relation d'équivalence* sur A est une relation $R \subseteq A \times A$ réflexive, symétrique et transitive.

La *classe d'équivalence* de $a \in A$ dans R est l'ensemble défini par

$$[a]_R \triangleq \{\, b \in A \mid aRb \,\}$$

Lorsqu'il n'y a pas d'ambiguité sur la relation R dont on parle, on écrit $[a]$ pour $[a]_R$.

Le *quotient* $A/_R$ est défini par :

$$A/_R \triangleq \{\, [a]_R \mid a \in A \,\}$$

c'est l'ensemble des classes d'équivalences de A.
L'*index* de R est le nombre de classes d'équivalence de R. Il est égal à $\#(A/_R)$ (cf. 0.5.1). □

0.3.7 Lemme Soit R une relation d'équivalence sur un ensemble A et $p, q \in A$, alors :

1. pRq ssi $[p] = [q]$.
2. Si $[p] \neq [q]$, alors $p \notin [q]$ et $q \notin [p]$.
3. $[p] = [q] \vee [p] \cap [q] = \emptyset$
4. $A = \bigcup_{r \in A} [r]$. □

0.3.8 Lemme Soit R, S deux équivalences sur A avec index fini et $R \subseteq S$.

1. $\forall p \in A \,.\, [p]_R \subseteq [p]_S$.
2. $\#(A/_R) \geq \#(A/_S)$. □

0.4 Fonctions

La notion de fonction est un cas particulier de la notion de relation binaire.

0.4.1 Définition (Fonction) Une *fonction partielle* de A dans B est un triplet $f = (A, B, R)$ où $R \subseteq A \times B$ est une relation, appelé le *graphe* de f, telle que

$$\forall a, b, b'. \big((a, b) \in R \wedge (a, b') \in R\big) \Rightarrow b = b'$$

On définit les ensembles suivants,

- $\mathrm{ED}(f) \triangleq A$, l'ensemble de départ de f,
- $\mathrm{EA}(f) \triangleq B$, l'ensemble d'arrivée de f,
- $\mathrm{dom}(f) \triangleq \{a \in A \mid \exists b \in B. (a, b) \in R\}$, le domaine (de définition) de f.
- $\mathrm{img}(f) \triangleq \{b \in B \mid \exists a \in A. (a, b) \in R\}$, l'image de f.

La fonction f est définie (resp. indéfinie) en $a \in A$ si $a \in \mathrm{dom}(f)$ (resp. $a \notin \mathrm{dom}(f)$).

La fonction f est totale si $\mathrm{dom}(f) = \mathrm{ED}(f)$. On dit aussi de f qu'elle est une application de A dans B.

L'ensemble des fonctions partielles de A dans B est noté $A \rightharpoonup B$. On note $A \to B$ l'ensemble des applications de A dans B. Remarquons que

$$(A \to B) \subseteq (A \rightharpoonup B) \subseteq \mathcal{P}(A \times B).$$

On écrit $f(a) = b$ ou $a \mapsto b$ si $(a, b) \in R$. □

Par abus de langage, on confond le graphe R d'une fonction $f = (A, B, R)$ avec f et on dit que f est une fonction, souvent sans préciser A ou B.

Souvent au lieu de noter $f \in A \to B$ nous écrivons $f : A \to B$. Pour définir les fonctions nous utilisons les notations suivantes toutes équivalentes.

$$f : x \mapsto x^2 \qquad f(x) \triangleq x^2 \qquad f \triangleq \lambda x.x^2$$

Pour spécifier l'ensemble de départ et d'arrivée de la fonction définie, nous écrivons,

$$\begin{array}{ccccc} f & : & A & \to & B \\ & & x & \mapsto & x^2 \end{array}$$

Une application $f : \mathbb{N} \to A$ est communément appelé *suite* sur A ou suite de A.

0.4.2 Définition (Égalité) Deux fonctions $f : A \rightharpoonup B$ et $g : A' \rightharpoonup B'$ sont égales (noté $f = g$) si :

1. $A = A'$ et $B = B'$,
2. $\mathrm{dom}(f) = \mathrm{dom}(g)$, et
3. $\forall a \in \mathrm{dom}(f)\,.\, f(a) = g(a)$.

0.4.3 Définition (Image d'un ensemble) Soit $f \in A \rightharpoonup B$.

Soit $X \subseteq A$, *l'image directe* de X par f est

$$f(X) \triangleq \{f(a) \mid a \in (X \cap \mathrm{dom}(f))\}$$

Soit $Y \subseteq B$, *l'image réciproque* de Y par f est

$$f^R(Y) \triangleq \{a \in \mathrm{dom}(f) \mid f(a) \in Y\}$$

□

0.4.4 Définition (Fonction injective, surjective, bijective) Une fonction f de A dans B est,

injective ssi $\forall a, a'.\, f(a) = f(a') \Rightarrow a = a'$

surjective ssi $\forall b \in B.\, \exists a \in A.\, f(a) = b$

bijective ssi f est injective et surjective. □

0.4.5 Lemme

Soit A et B deux ensembles non vides.

1. Si $f : A \to B$ est une application injective,
   alors il existe une application $g : B \to A$ qui est surjective.
2. Si $g : B \to A$ est une application surjective,
   alors il existe une application $f : A \to B$ qui est injective.
3. Soit $f : A \to B$ une application, f^{-1} est une application
   ssi f est injective. □

0.4.6 Définition (Application involutive, idempotente) Soit $f : A \to A$ une application.

- f est *involutive* ssi $f \circ f = \mathrm{id}_A$.
- f est *idempotente* ssi $f \circ f = f$. □

0.4.7 Définition (Fermeture) Soit $(X, \sqsubseteq)$ un ordre. Une application $f : X \to X$ est une *fermeture* (sur X) si pour tout $x, y \in X$:

1. $x \sqsubseteq f(x)$,
2. si $x \sqsubseteq y$ alors $f(x) \sqsubseteq f(y)$,
3. $f(f(x)) = f(x)$

Un élément x est un *point fixe* de f si $x = f(x)$. □

0.4.8 Définition (Stabilité) Soit $f : X^n \to X$ une application. Un sous-ensemble $Y \subseteq X$ est *stable par* f si :

$$\forall y_1 \ldots, y_n \in Y\,.\, f(y_1 \ldots, y_n) \in Y$$

0.5 Cardinalité

0.5.1 Définition (Taille d'un ensemble) Soit A un ensemble. On dit que A est *fini* s'il existe $n \in \mathbb{N}$ tel qu'il existe une application bijective de A dans $[1, n]$. Si un tel n existe, il est unique et est appelé la taille de l'ensemble A, que l'on notera $\#(A)$. Si A n'est pas fini, on dit que A est *infini* et on pose $\#(A) = \infty$. □

Si, pour les ensembles finis, il est facile de comparer leur taille, pour les ensembles infinis, on introduit la notion de *cardinal* pour les comparer.

0.5.2 Définition (Cardinalité) Soit A et B deux ensembles.

1. A et B ont la même cardinalité, $\mathrm{card}(A) = \mathrm{card}(B)$, s'il existe une application bijective de A dans B. On dit aussi que A et B sont *équipotents*.
2. A a une cardinalité plus petite que celle de B, $\mathrm{card}(A) \leq \mathrm{card}(B)$, s'il existe une application injective de A dans B.
3. A a une cardinalité strictement plus petite que celle de B, $\mathrm{card}(A) < \mathrm{card}(B)$, si $\mathrm{card}(A) \leq \mathrm{card}(B)$ mais $\mathrm{card}(A) \neq \mathrm{card}(B)$.

Il est possible de reformuler les comparaisons de cardinalité en termes d'applications surjectives.

0.5.3 Définition (Dénombrable) Soit A un ensemble.

1. A est *dénombrable* si A est fini ou équipotent à $\mathbb{N}$.
2. A est *infiniment dénombrable* si A est infini et dénombrable.
3. A est *non-dénombrable* si $\mathrm{card}(\mathbb{N}) < \mathrm{card}(A)$.

0.5.4 Théorème (Cantor) Soit A un ensemble. Alors $\mathrm{card}(A) < \mathrm{card}(\mathcal{P}(A))$.

0.6 Structures algébriques

0.6.1 Définition (Monoïde) Soit M un ensemble et op une application de $M \times M$ dans M (aussi appelé loi de composition interne). Le couple (M, op) est un *monoïde* si :

- op est *associative* :

$$\forall x, y, z \in M : \mathrm{op}(x, \mathrm{op}(y, z)) = \mathrm{op}(\mathrm{op}(x, y), z)$$

- op admet un *élément neutre* :

$$\exists e \in M : \forall x \in M : \mathrm{op}(e, x) = \mathrm{op}(x, e) = x$$

0.6.2 Lemme (Unicité de l'élément neutre) Soit (M, op) un monoïde et soit $e, e' \in M$ deux éléments neutres pour op. Alors $e = e'$.

On a donc que si (M, op) est un monoïde, il existe un unique élément neutre pour op appelé l'élément neutre de (M, op). Si e est cet élément neutre, on pourra aussi dire que (M, op) est un monoïde d'élément neutre e.

Si (M, op) est un monoïde, il est d'usage de noter de manière infixe la loi de composition interne : $\mathrm{op}(x, y)$ est plutôt noté $x \,\mathrm{op}\, y$. Ainsi, l'associativité de op s'écrit alors $\forall x, y, z \in M : x \,\mathrm{op}(y \,\mathrm{op}\, z) = (x \,\mathrm{op}\, y) \,\mathrm{op}\, z$.

0.6.3 Définition (Puissance d'un élément) Soit (M, op) un monoïde d'élément neutre e. On définit pour $x \in M$, la puissance n^{e} d'un élément, pour $n \in \mathbb{N}$, comme suit :

$$x^0 \triangleq e$$
$$x^{n+1} \triangleq x \,\mathrm{op}\, x^n$$

On a donc $x^n = \underbrace{x \,op \cdots \mathrm{op}\, x}_{n \text{ fois}}$.

0.6.4 Définition (Monoïde commutatif) Soit (M, op) un monoïde. Le couple (M, op) est dit *commutatif* si

– op est *commutative* :

$$\forall x, y \in M : x \,\mathrm{op}\, y = y \,\mathrm{op}\, x$$

La loi de composition interne op d'un monoïde commutatif est souvent noté $+$ et l'élément neutre $\mathbf{0}$. Si la loi est noté $+$, on note généralement nx la puissance n^{e} de x.

Un exemple de monoïde commutatif est $(\mathbb{N}, +)$ où $+$ est l'addition classique sur les entiers naturels. L'élément neutre de $(\mathbb{N}, +)$ est bien entendu 0.

0.6.5 Définition (Groupe) Soit G un ensemble muni d'une loi de composition interne $\mathrm{op} : G \times G \to G$. Le couple (G, op) est un groupe si :

– (G, op) est un monoïde d'élément neutre e,

– Chaque élément de G admet un *symétrique* à gauche et à droite :

$$\forall x \in G : \exists y \in G : x \,\mathrm{op}\, y = y \,\mathrm{op}\, x = e$$

De plus, le groupe (G, op) est dit *abélien* (ou commutatif) si op est commutative.

0.6.6 Lemme (Unicité du symétrique) Soit (G, op) un groupe d'élément neutre e et $x, y, y' \in G$ tels que $x \,\mathrm{op}\, y = y \,\mathrm{op}\, x = e$, $x \,\mathrm{op}\, y' = y' \,\mathrm{op}\, x = e$. Alors $y = y'$.

Le lemme précédent dit que chaque élément x d'un groupe admet un unique élément symétrique, que l'on notera généralement x^{-1} (ou $-x$ si on utilise $+$ pour dénoter la loi de composition interne du groupe abélien).

Notons aussi qu'il est possible de prendre une définition de groupe ne requérant seulement l'existence d'un symétrique à gauche pour chaque

élément. C'est un bon exercice de montrer que cette définition en apparence moins forte coïncide avec celle donnée ci-dessus.

Le couple $(\mathbb{Z}, +)$ est un exemple de groupe commutatif (où $+$ est l'addition classique sur les entiers relatifs) d'élément neutre 0. En revanche $(\mathbb{N}, +)$ n'est pas un groupe car tous les éléments distincts de 0 n'ont pas de symétrique.

Chapitre 1

Introduction

$Id: notes-1.tex,v 1.16 2005/01/27 10:18:00 jobo Exp $

semaine 1
lundi &
mercredi

1.1 Alphabets et mots

1.1.1 Définition (Alphabet) On appelle *alphabet* tout ensemble fini Σ. Les éléments d'un alphabet sont traditionnellement appelés *symboles*, *lettres* ou *caractères*. □

Pour un alphabet $\Sigma \triangleq \{ s_1, s_2, \ldots, s_k \}$, on considère souvent l'ordre total $\preceq$ défini par $s_i \preceq s_j$ si et seulement si $i \leq j$.

1.1.2 Définition (Mots) Un *mot* w sur un alphabet Σ est une séquence finie de lettres de Σ.

Autrement dit, un mot w est un n-uplet $(a_1, a_2, \ldots, a_n)$ de lettres de Σ où $n \in \mathbb{N}$ est appelé la *longueur* de w, notée $|w|$. Si $n = 0$, w est l'unique mot de longueur nulle appelé *mot vide* que l'on note ϵ . La i^e *projection* $(w)_i$ de w est la lettre a_i, pour $1 \leq i \leq n$.

L'ensemble des mots sur un alphabet Σ est noté Σ^*. L'ensemble des mots non vides, c'est à dire $\Sigma^* \setminus \{\epsilon\}$ est noté Σ^+. □

Par convention, nous utilisons les (meta-) variables $a, b, c, \ldots$ pour les lettres et $\ldots, u, v, w, x, y, z$ les mots.

1.1.3 Définition (Concaténation de mots) Soit $w \triangleq (a_1, \ldots, a_n) \in \Sigma^*$ et $w' \triangleq (b_1, \ldots, b_m) \in \Sigma^*$, la *concaténation* $w \cdot w'$ de w avec w' est définie par,

$$w \cdot w' \triangleq (a_1, \ldots, a_n, b_1, \ldots, b_m)$$

□

1.1.4 Théorème $(\Sigma^*, \cdot)$ est un monoïde d'élément neutre ϵ.

1.1.5 Notation Pour un alphabet $\Sigma \triangleq \{s_1, \ldots, s_n\}$ on identifie la lettre $s_i \in \Sigma$ avec le mot $(s_i) \in \Sigma^*$ de longueur 1. Ceci nous permet d'écrire pour $w \triangleq (a_1, a_2, \ldots, a_n) \in \Sigma^*$, $w = a_1 \cdot a_2 \cdot \ldots \cdot a_n = a_1 a_2 \ldots a_n$ □

1.1.6 Définition (Préfixe, suffixe, facteur) Soit $w \in \Sigma^*$ un mot sur un alphabet Σ.

- $u \in \Sigma^*$ est un *préfixe* de w s'il existe $v \in \Sigma^*$ tel que $w = u \cdot v$.
- $v \in \Sigma^*$ est un *suffixe* de w s'il existe $u \in \Sigma^*$ tel que $w = u \cdot v$.
- $w' \in \Sigma^*$ est un *facteur* de w s'il existe $u, v \in \Sigma^*$ tel que $w = u \cdot w' \cdot v$.

1.1.7 Lemme (Décomposition d'un mot) Soit w un mot sur un alphabet Σ , nous avons,

Soit $w = \epsilon$

ou alors $\exists a \in \Sigma, w' \in \Sigma^*. w = a \cdot w'$ avec $|w'| = |w| - 1$ □

1.1.8 Lemme (Principe d'induction sur les mots) Soit $P(w)$ un prédicat sur les mots d'un alphabet Σ.

Si $P(\epsilon)$

et $\forall w \in \Sigma^*. P(w) \Rightarrow \forall a \in \Sigma. P(a \cdot w)$

alors $\forall w \in \Sigma^*. P(w)$. □

Remarquons que les deux derniers lemmes peuvent se reformuler en décomposant les mots par la droite.
Si le dernier lemme nous permet de montrer qu'un prédicat est vrai sur l'ensemble des mots, il nous permet aussi de justifier les définitions par induction structurelle sur les mots en définissant

- le cas de base : pour le mot vide ϵ
- le cas inductif : supposant avoir défini pour le mot $w \in \Sigma^*$, on définit pour les mots $a \cdot w$ où $a \in \Sigma$.

Par exemple, on peut définir la longueur $\mathsf{len}(w)$ d'un mot w par induction structurelle en définissant :

- le cas de base. On définit $\mathsf{len}(\epsilon) \triangleq 0$
- le cas inductif. Soit $w \in \Sigma^*$ et supposons que $\mathsf{len}(w)$ soit défini et égal à n. On définit alors pour tout $a \in \Sigma$, $\mathsf{len}(a \cdot w) \triangleq n + 1 = \mathsf{len}(w) + 1$.

On peut alors montrer que $\mathsf{len}(w)$ et $|w|$ sont égaux pour tous mots $w \in \Sigma^*$ (par induction sur w !).

Ce genre de définition par induction sur les mots étant fréquent, on utilisera la présentation sous forme de *règles d'inférence*.

En continuant sur le même exemple, cela donnerait :

$$\frac{}{\mathsf{len}(\epsilon) \triangleq 0} \qquad \frac{\mathsf{len}(w) = n}{\mathsf{len}(a \cdot w) \triangleq n + 1}$$

Ces règles d'inférence se lisent : en supposant les prémisses (ce qui se trouve au-dessus de la barre), on définit la conclusion (ce qui se trouve en-dessous de la barre). S'il n'y a pas de prémisses, on parle de règle axiome (ou plus simplement axiome).

L'ordre total d'un alphabet Σ induit des ordres sur les mots de Σ^*.

1.1.9 Définition (Ordre sur les mots) Soit un alphabet Σ et un ordre total $(\Sigma, \preceq)$ (et l'ordre strict induit $\prec$).

Ordre alphabétique. L'ordre alphabétique $(\Sigma^*, \ll_{\mathrm{d}})$ est la plus petite relation sur Σ^* qui satisfait les règles suivantes.

$$\mathrm{D}_1 \ \frac{}{\epsilon \ll_{\mathrm{d}} w} \qquad \mathrm{D}_2 \ \frac{}{a \cdot w \ll_{\mathrm{d}} a' \cdot w'} \ a \prec a'$$

$$\mathrm{D}_3 \ \frac{w \ll_{\mathrm{d}} w'}{a \cdot w \ll_{\mathrm{d}} a \cdot w'}$$

Ordre lexicographique. L'ordre lexicographique $(\Sigma^*, \ll_{\mathrm{l}})$ est la plus petite relation sur Σ^* qui satisfait les règles suivantes.

$$\mathrm{L}_1 \ \frac{}{\epsilon \ll_{\mathrm{l}} w} \qquad \mathrm{L}_2 \ \frac{}{w \cdot a \ll_{\mathrm{l}} w \cdot a'} \ a \preceq a'$$

$$\mathrm{L}_3 \ \frac{w \ll_{\mathrm{l}} w'}{w \cdot a \ll_{\mathrm{l}} w' \cdot a'} \ w \neq w'$$

L'ordre lexicographique ordonne les mot d'abord par leur taille puis, si celle-ci est égale, alphabétiquement. □

1.1.10 Théorème

1. L'ordre alphabétique est total.
2. L'ordre lexicographique est total. □

1.2 Langages

1.2.1 Définition (Langage) On appelle *langage* sur un alphabet Σ tout sous-ensemble de Σ^*. Un langage n'est donc rien d'autre qu'un ensemble de mots. □

Nous utilisons les meta-variables $A, B, C \ldots, L, \ldots$ pour les langages. Les deux langages $\emptyset$ et $\{\epsilon\}$ sont des langages sur n'importe quel alphabet.

Pour construire des langages à partir d'autres langages, nous utilisons notamment les opérations suivantes.

1.2.2 Définition (Opération sur les langages) Soit Σ un alphabet fini, L et L' deux langages sur Σ^*.

Union. L'union $L \cup L'$ de L et L' correspond à leur union ensembliste.

Intersection. L'intersection $L \cap L'$ de L et L' correspond à leur intersection ensembliste.

Complément. Le complément $\overline{L}$ de L est le complément absolu de L par rapport à Σ^* (i.e. $\overline{L} = \Sigma^* \backslash L$) .

Concaténation. La concaténation LL' de L et L' est définie par $LL' \triangleq \{ww' \mid w \in L \wedge w' \in L'\}$.

Itération. La n^e itération L^n d'un language n est définie de manière inductive par,

$$L^0 \triangleq \{\epsilon\} \qquad L^{n+1} \triangleq LL^n$$

Fermeture itérative. La fermeture itérative (ou de Kleene) L^* de L est définie par

$$L^* \triangleq \bigcup_{n\in\mathbb{N}} L^n$$

On utilise aussi la notation suivante, $L^+ \triangleq LL^*$.

1.2.3 Lemme

1. Propriétés de la fermeture de Kleene.

$$L^*L^* = L^* \quad L^{**} = L^* \quad \emptyset^* = \{\,\epsilon\,\}$$

□

1.3 Fonctions versus programmes

Étant donné un langage de programmation quelconque **X** (exécuté de façon déterministe), nous démontrons qu'il existe plus de fonctions sur $\mathbb{N}$ que de programmes de **X** pouvant calculer des fonctions sur $\mathbb{N}$.

1.3.1 Définition L'ensemble $\mathbf{F}_\mathbb{N}$ de toutes les fonctions totales sur $\mathbb{N}$ est défini par :

$$\mathbf{F}_\mathbb{N} \triangleq \{\, f \mid f : \mathbb{N} \to \mathbb{N} \,\}$$

1.3.2 Définition Soit Σ l'alphabet d'un langage de programmation **X**. L'ensemble $\mathbf{P}_\mathbf{X}$ des mots/programmes sur Σ (voir §1.1 et §1.2) est défini par :

$$\mathbf{P}_\mathbf{X} \triangleq \Sigma^*$$

1.3.3 Définition Soit $\mathrm{exec}_\mathbf{X} : \mathbf{P}_\mathbf{X} \rightharpoonup (\mathbb{N} \to \mathbb{N})$ un interpréteur de **X** qui associe à un programme $\mathtt{p}$ une fonction $\mathrm{exec}_\mathbf{X}(\mathtt{p}) : \mathbb{N} \to \mathbb{N}$. Notons que $\mathrm{exec}_\mathbf{X}$ est partielle, tous les programmes ne sont pas associés à une fonction. Une fonction $f : \mathbb{N} \to \mathbb{N}$ est dite *calculable* dans le langage **X** si $f \in \mathrm{img}(\mathrm{exec}_\mathbf{X})$, c'est à dire si

$$\exists \mathtt{p} \in \mathbf{P}_\mathbf{X} \,.\, \mathrm{exec}_\mathbf{X}(\mathtt{p}) = f$$

Nous écrivons

$$\mathbf{F}_\mathbf{X} \triangleq \{\, f : \mathbb{N} \to \mathbb{N} \mid f \text{ calculable par } \mathbf{X} \,\} \qquad (\subseteq \mathbf{F}_\mathbb{N})$$

l'ensemble de fonctions calculables par (les programmes) X.

1.3.4 Théorème Pour tout **X** : $\mathrm{card}(\mathbf{F}_\mathbf{X}) < \mathrm{card}(\mathbf{F}_\mathbb{N})$.

Nous décomposons la preuve comme suit :

$$\mathrm{card}(\mathbf{F}_\mathbf{X}) \overset{(0)}{\leq} \mathrm{card}(\mathbf{P}_\mathbf{X}) \overset{(1)}{\leq} \mathrm{card}(\mathbb{N}) \overset{(2)}{<} \mathrm{card}(\mathcal{P}(\mathbb{N})) \overset{(3)}{\leq} \mathrm{card}(\mathbf{F}_\mathbb{N})$$

1.3.5 Lemme (Partie (0) de la preuve de 1.3.4) $\mathrm{card}(\mathbf{F_X}) \leq \mathrm{card}(\mathbf{P_X})$

1.3.6 Lemme (Partie (1) de la preuve de 1.3.4) $\mathrm{card}(\mathbf{P_X}) \leq \mathrm{card}(\mathbb{N})$

1.3.7 Lemme (Partie (2) de la preuve de 1.3.4) $\mathrm{card}(\mathbb{N}) < \mathrm{card}(\mathcal{P}(\mathbb{N}))$

1.3.8 Lemme (Partie (3) de la preuve de 1.3.4) $\mathrm{card}(\mathcal{P}(\mathbb{N})) \leq \mathrm{card}(\mathbf{F}_{\mathbb{N}})$

1.3.9 Théorème Supposons qu'il existe une énumeration $f_0, f_1, f_2, \ldots$ de toutes les fonctions sur les nombres naturels. Définissons :

$$\mathrm{diag}(i) \triangleq f_i(i)$$

Alors, la fonction définie par

$$g(i) \triangleq \mathrm{diag}(i) + 1$$

n'apparaît pas dans cette énumeration.