

Théorie des types : introduction et utilisation en Lean.

Dorian Guillet

24 avril 2025

Table des matières

1	Théorie des Types	3
1.1	Introduction	3
1.2	Règles structurelles	4
1.2.1	Contexte	4
1.2.2	Égalité	4
1.3	Construction de types	5
1.3.1	Univers	5
1.3.2	Fonctions	5
1.3.3	Fonctions dépendantes (Π -type)	7
1.3.4	Produits	8
1.3.5	Paires dépendantes (Σ -types)	8
1.3.6	Type vide	9
1.3.7	Type unité	10
1.3.8	Coproduit	10
1.3.9	Types inductifs : W-types	12
1.3.10	Entiers naturels	14
1.3.11	Listes	16
1.4	Correspondance de Curry-Howard	18
2	Formalisation du théorème de Bowen en Lean	19
2.1	Formalisation de l'énoncé du théorème	19
2.2	Preuve d'un résultat topologique	20
3	Topologie des espaces ultramétriques	22

1 Théorie des Types

1.1 Introduction

La théorie des types se veut être une alternative à la théorie des ensembles de Zermelo-Fraenkel (ZF). Or les fondations de cette dernière s'appuient sur le système déductif de la logique du premier ordre, et la théorie des ensembles est formulée à l'intérieur de ce système, donc cette théorie est formée de deux couches : la logique du premier ordre, puis la théorie des ensembles, formée de ses axiomes. On a donc deux objets fondamentaux dans cette approche : les propositions (qui se basent sur la logique du premier ordre) et les ensembles de ZF.

Pour éviter cette construction en deux couches, la théorie des types possède son propre système déductif, par conséquent une fois les jugements et les règles du système déductif définies, il est prêt à être utilisé sans axiomes supplémentaires. Ainsi, cette théorie ne possède qu'un objet fondamental : les **types**.

Ayant uniquement des types, pour pouvoir formuler des théorèmes on a besoin de l'équivalent des propositions qui sont ici des types particulier, dont la construction suit des règles qui seront précisées après. Dans cette théorie, prouver un théorème est donc équivalent à construire un objet qui serait un élément du type correspondant au théorème (ici l'objet en question est une preuve).

On peut aussi voir les types d'un point de vue plus proche de la théorie des ensembles, en interprétant le fait qu'un élément a soit de type A comme l'affirmation $a \in A$. Cependant ici l'affirmation $a \in A$ est une proposition alors que dire " a est de type A " (que l'on notera dorénavant $a : A$) est un jugement. En effet, dans la théorie des types un élément possède toujours un type (uniquement) déterminé.

Le système déductif de cette théorie est composé de trois jugements :

1. **Jugement de typage** $a : A$, qui affirme que a est de type A .
2. **Jugement d'égalité** $a \equiv b : A$, qui affirme que a et b sont égaux par définition dans le type A .
3. **Jugement de contexte** $\Gamma \text{ ctx}$, exprimant le fait que Γ est un contexte bien formé.

A noter que le symbole " \equiv " est différent de " $=$ ". En effet, si $a, b : A$, alors on a le type $a =_A b$ qui correspond à une égalité que l'on peut prouver, c'est l'égalité propositionnelle. Pour l'égalité "par définition" du système déductif, la prouver ou la supposer n'a pas réellement de sens étant donné qu'elle est vrai par définition (ou par construction).

Cette distinction entre proposition et jugement est fondamentale. Un jugement est une affirmation dans le système déductif de la théorie, qui est donc considéré comme vrai et n'est pas à prouver, alors qu'une proposition est un type, pouvant être non vide et se situe donc dans la théorie elle-même.

1.2 Règles structurelles

Pour prouver une proposition dans la théorie des types, on utilise des règles d'inférences, ou plus simplement règles, de la forme

$$\frac{\mathcal{I}_1 \quad \dots \quad \mathcal{I}_k}{\mathcal{I}} \text{NOM}$$

où \mathcal{I} est la conclusion de la règle tandis que les $\mathcal{I}_1, \dots, \mathcal{I}_k$ sont les prémisses ou hypothèses de la règle.

Avec de telles règles, on peut prouver une proposition en construisant un arbre de preuve dont la racine est la proposition à prouver et les liens entre les feuilles respectent les règles d'inférence de la théorie.

1.2.1 Contexte

Les règles concernant le jugement de contexte sont au nombre de deux et permettent de vérifier qu'un contexte Γ est bien formé, c'est-à-dire que toutes les variables et jugements apparaissant dans Γ sont dans un ordre cohérent. Pour ce faire on a ces règles :

$$\frac{}{\cdot \text{ ctx}} \emptyset \text{ ctx} \qquad \frac{a_1 : A_1, \dots, a_{n-1} : A_{n-1} \vdash A_n \text{ type}}{(a_1 : A_1, \dots, a_n : A_n) \text{ ctx}} \text{ ctx}$$

Le jugement $A_n \text{ type}$ signifie que A_n est un type et sera détaillé davantage dans la section suivante. La première règle dit qu'un contexte vide est toujours bien formé, la seconde règle dit que un contexte est bien formé dès lors que la dernière variable est bien typé sous l'hypothèse que le contexte auquel on retire la dernière variable est lui-même bien formé.

1.2.2 Égalité

L'égalité par définition " \equiv " se comporte comme l'égalité classique, pour se faire elle vérifie les mêmes propriétés élémentaires, à savoir la réflexivité, la symétrie et la transitivité que l'on exprime avec les règles suivantes.

$$\frac{\Gamma \vdash a : A}{\Gamma \vdash a \equiv a : A} \text{ refl} \qquad \frac{\Gamma \vdash b \equiv a : A}{\Gamma \vdash a \equiv b : A} \text{ sym} \qquad \frac{\Gamma \vdash a \equiv b : A \quad \Gamma \vdash b \equiv c : A}{\Gamma \vdash a \equiv c : A} \text{ trans}$$

On ajoute aussi deux règles supplémentaires qui permettent d'échanger le rôle de deux élément ou type sous l'hypothèse qu'ils sont égaux.

$$\frac{\Gamma \vdash a : A \quad \Gamma \vdash A \equiv B}{\Gamma \vdash a : B} \equiv \text{ type} \qquad \frac{\Gamma \vdash a \equiv b : A \quad \Gamma \vdash A \equiv B}{\Gamma \vdash a \equiv b : B} \equiv \text{ eq}$$

Enfin, on ajoute une dernière règle permettant d'utiliser des jugements présent dans le contexte, qui s'exprime sous la forme suivante.

$$\frac{(a_1 : A_1, \dots, a_n : A_n) \text{ ctx}}{a_1 : A_1, \dots, a_n : A_n \vdash a_i : A_i} \text{ var}$$

1.3 Construction de types

Pour construire un nouveau type à partir d'autres, on doit donner 3 règles :

- **Formation du type**, qui permet de construire un type à partir d'autres types ou famille de types,
- **Introduction**, qui explique comment sont construits les éléments de ce type,
- **Élimination**, décrivant comment utiliser ces éléments.

Partant de ces 3 règles, on peut construire un type et éventuellement ajouter des règles supplémentaires concernant leur comportement par rapport à l'égalité par définition.

1.3.1 Univers

Plus tôt, on a utilisé un jugement de la forme " $\Gamma \vdash A$ type" pour signifier que A est un type. Cependant ce jugement n'est pas un jugement de la théorie, on se ramène alors à un autre jugement déjà présent : le jugement de typage. Pour ce faire, on doit introduire un type composé de type, un type univers \mathcal{U} . Pour la même raison, on voudrais dire que \mathcal{U} est lui-même un élément d'un type plus grand et ainsi de suite. Pour résoudre ce problème, on postule qu'il existe une hiérarchie de type

$$\mathcal{U}_0, \mathcal{U}_1, \mathcal{U}_2, \dots, \mathcal{U}_i, \dots$$

telle que $\mathcal{U}_i : \mathcal{U}_{i+1}$.

Pour ces types, on a seulement une règle d'introduction et une règle décrivant la hiérarchie entre ces types :

$$\frac{\Gamma \text{ ctx}}{\Gamma \vdash \mathcal{U}_i : \mathcal{U}_{i+1}} (\mathcal{U} \text{ i}) \qquad \frac{\Gamma \vdash A : \mathcal{U}_i}{\Gamma \vdash A : \mathcal{U}_{i+1}} (\mathcal{U} \text{ cumul})$$

Par conséquent, la règle sur les contextes devient la suivante :

$$\frac{(a_1 : A_1, \dots, a_{n-1} : A_{n-1}) \vdash A_n : \mathcal{U}_k}{(a_1 : A_1, \dots, a_n : A_n) \text{ ctx}} (\text{ctx})$$

1.3.2 Fonctions

Étant donné deux types $A, B : \mathcal{U}$, on peut former le type des fonctions de A dans B noté $A \rightarrow B$ grâce à la règle de formation suivante :

$$\frac{\Gamma \vdash A : \mathcal{U}_i \quad \Gamma \vdash B : \mathcal{U}_i}{\Gamma \vdash A \rightarrow B : \mathcal{U}_i} (\rightarrow \text{ f})$$

Une fonction est donc un élément f de type $A \rightarrow B$. Si on se donne $a : A$, on peut évaluer f en a ce qui donne un élément de type B que l'on note $f \ a$ ou bien $f(a)$ qui est appelé valeur de f en a , c'est la règle d'élimination de \rightarrow :

$$\frac{\Gamma \vdash f : A \rightarrow B \quad \Gamma \vdash a : A}{\Gamma \vdash f a : B} (\rightarrow e)$$

Pour former une fonction f de A dans B *ie.* un élément de type $A \rightarrow B$, la manière canonique de faire est d'utiliser les λ -abstraction et la règle d'introduction suivante :

$$\frac{\Gamma, x : A \vdash \Phi : B}{\Gamma \vdash \lambda(x : A).\Phi : A \rightarrow B} (\rightarrow i)$$

Dans cette règle Φ correspond à une formule qui peut éventuellement faire intervenir la variable x .

Enfin, lorsque l'on considère une fonction $f : A \rightarrow B$ définie par $f \equiv \lambda(x : A).\Phi$ où Φ est une formule et un élément $a : A$, il est naturel que la valeur de f en a soit égale à la formule Φ où l'on remplace les occurrences de x par des a , ce que l'on note $\Phi[a/x]$. Ce comportement est en fait une règle d'égalité que l'on peut énoncer sous cette forme :

$$\frac{\Gamma, x : A \vdash \Phi : B \quad \Gamma \vdash a : A}{\Gamma \vdash (\lambda(x : A).\Phi) a \equiv \Phi[a/x]} (\beta)$$

Exemple. Considérons un type $A : \mathcal{U}$ et la fonction "identité" de A définie par $I \equiv \lambda(x : A).x$. Pour prouver que le type de I est bien $A \rightarrow A$, on peut utiliser les règles énoncées précédemment :

$$\frac{\frac{A : \mathcal{U} \vdash A : \mathcal{U}}{A : \mathcal{U}, x : A \vdash x : A}}{A : \mathcal{U} \vdash \lambda(x : A).x : A \rightarrow A}$$

On a vu jusqu'ici comment construire des fonctions à une variable, on peut alors généraliser pour obtenir des fonctions à plusieurs variables. Pour ce faire, considérons trois types $A, B, C : \mathcal{U}$. Naïvement, on voudrais construire une fonction de type $A \times B \rightarrow C$, mais le type $A \times B$ n'est pas encore défini. Pour contourner ce problème, on peut voir une fonction f de $A \times B \rightarrow C$ comme

$$f(x, y) = (\lambda(a : A).f(a, y))x = ((\lambda(a : A).(\lambda(b : B).f(a, b))) x) y \quad (1)$$

$$= (\lambda(a : A).\lambda(b : B).f(a, b)) x y. \quad (2)$$

On a ainsi obtenu une fonction de type $A \rightarrow B \rightarrow C$ qui prend les mêmes valeurs que f grâce à ce processus de *curryfication*.

Exemple. Considérons deux types $A, B : \mathcal{U}$ et la fonction K définie par

$$K \equiv \lambda(x : A).(\lambda(y : B).x)$$

Grâce à un arbre similaire au précédent, on trouve que le type de K est $A \rightarrow B \rightarrow A$ (on omet les parenthèses en prenant comme convention que $A \rightarrow A \rightarrow A$ est égal à $A \rightarrow (A \rightarrow A)$). De

plus, on peut également montrer que si $a : A$ et $b : B$, alors $K a b \equiv a$. En effet, A FAIRE.

Si on considère deux types $A, B : \mathcal{U}$ et qu'on les voit comme des propositions, alors le type $A \rightarrow B$ peut s'interpréter comme l'implication $A \implies B$.

1.3.3 Fonctions dépendantes (Π -type)

Une manière de généraliser le type des fonctions est de définir un type de fonctions dépendantes (ou Π -type), qui est un type de fonction dont le codomaine dépend du point d'application de la fonction.

Pour former ce nouveau type, on considère $A : \mathcal{U}$ un type et $B : A \rightarrow \mathcal{U}$ une famille de type indexée sur A . On peut alors former le type $\prod_{a:A} B(a)$ grâce à la règle de formation suivante :

$$\frac{\Gamma \vdash A : \mathcal{U}_i \quad \Gamma, a : A \vdash B(a) : \mathcal{U}_i}{\Gamma \vdash \prod_{a:A} B(a) : \mathcal{U}_i} (\Pi f)$$

On construit des éléments de type $\prod_{a:A} B(a)$ de manière analogue aux fonctions en utilisant des λ -abstractions. En effet, $\lambda(a : A). \Phi$ est de type $\prod_{a:A} B(a)$ si lorsque $a : A$, alors $\Phi : B(a)$. Cette règle énoncé plus formellement est la règle d'introduction de ce nouveau type :

$$\frac{\Gamma, a : A \vdash \Phi : B(a)}{\Gamma \vdash \lambda(a : A). \Phi : \prod_{a:A} B(a)} (\Pi i)$$

Ensuite, la règle d'élimination est similaire à celle des types de fonctions. Si on considère $f : \prod_{a:A} B(a)$ et $a : A$, alors $f a$ est de type $B(a)$, ce que l'on peut traduire avec la règle suivante :

$$\frac{\Gamma \vdash f : \prod_{a:A} B(a) \quad \Gamma \vdash a : A}{\Gamma \vdash f a : B(a)} (\Pi e)$$

Également, la règle β des fonctions se généralise au Π -type :

$$\frac{\Gamma, x : A \vdash \Phi : B(x) \quad \Gamma \vdash a : A}{\Gamma \vdash (\lambda(x : A). \Phi) a \equiv \Phi[a/x]} (\beta)$$

L'utilité des types de fonctions dépendantes est notamment de pouvoir définir des fonctions de façon polymorphes, comme le montre les exemples suivants.

Exemple. La fonction identité du paragraphe précédent était défini sur un type $A : \mathcal{U}$ quelconque. On peut alors généraliser sa définition de la manière suivante :

$$I \equiv \lambda(A : \mathcal{U}). \lambda(a : A). a : \prod_{A:\mathcal{U}} A \rightarrow A.$$

Ainsi définie, la fonction I ne dépend pas d'un type préexistant.

On peut également redéfinir la fonction constante K d'une manière analogue :

$$K \equiv \lambda(A : \mathcal{U}). \lambda(B : \mathcal{U}). \lambda(x : A). \lambda(y : B). x : \prod_{A : \mathcal{U}} \prod_{B : \mathcal{U}} A \rightarrow B \rightarrow A.$$

Pour ces types et définition polymorphe, on peut également avoir la notation I_A à la place de $I A$ pour plus de clarté.

D'un autre point de vue ce type peut également être vu comme l'équivalent du \forall de la logique du première ordre. En effet, si on considère $A : \mathcal{U}$ un type et $C : A \rightarrow \mathcal{U}$ une famille de type, que l'on peut également voir comme un prédicat, alors le type $\prod_{a:A} C(a)$ se comporte comme la proposition $\forall a, C(a)$ en logique classique.

1.3.4 Produits

Etant donné deux types $A, B : \mathcal{U}_i$, comme en théorie des ensembles on veut construire le type $A \times B$ des paires d'éléments de A et de B . Pour construire ce type on a la règle de formation suivante :

$$\frac{\Gamma \vdash A : \mathcal{U}_i \quad \Gamma \vdash B : \mathcal{U}_i}{\Gamma \vdash A \times B : \mathcal{U}_i} (\times \text{ f})$$

Les éléments de ce type sont des paires d'éléments et sont donc de la forme $(a, b) : A \times B$ où $a : A$ et $b : B$, on a donc la règle d'introduction pour décrire les paires :

$$\frac{\Gamma \vdash a : A \quad \Gamma \vdash b : B}{\Gamma \vdash (a, b) : A \times B} (\times \text{ i})$$

Ensuite pour les règles d'éliminations et de calculs, on introduit deux fonctions $\pi_1 : A \times B \rightarrow A$ et $\pi_2 : A \times B \rightarrow B$ qui projette un élément $(a, b) : A \times B$ sur A et sur B .

$$\begin{array}{cc} \frac{\Gamma \vdash e : A \times B}{\Gamma \vdash \pi_1 e : A} (\times_1 \text{ e}) & \frac{\Gamma \vdash e : A \times B}{\Gamma \vdash \pi_2 e : B} (\times_2 \text{ e}) \\[10pt] \frac{\Gamma \vdash a : A \quad \Gamma \vdash b : B}{\Gamma \vdash \pi_1 (a, b) \equiv a} (\times_1 \equiv) & \frac{\Gamma \vdash a : A \quad \Gamma \vdash b : B}{\Gamma \vdash \pi_2 (a, b) \equiv b} (\times_2 \equiv) \end{array}$$

Enfin, pour les types produits on a également une règle d'unicité reliant un élément à ses projections :

$$\frac{\Gamma \vdash e : A \times B}{\Gamma \vdash e \equiv (\pi_1 e, \pi_2 e)} (\times \text{ u})$$

On peut également voir les types produits comme un cas particulier des types de fonctions dépendantes dont le domaine est le type fini **2** à deux éléments qui seront décrit dans 1.3.8.

1.3.5 Paires dépendantes (Σ -types)

Si on considère un type $A : \mathcal{U}_i$ et une famille de type $B : A \rightarrow \mathcal{U}_i$ indexée sur A , on veut pouvoir construire l'union disjointe des $B(a)$ pour $a : A$. Pour ce faire, on introduit les types de

paires dépendantes (où Σ -type) qui se forme grâce à la règle :

$$\frac{\Gamma \vdash A : \mathcal{U}_i \quad \Gamma, a : A \vdash B(a) : \mathcal{U}_i}{\Gamma \vdash \Sigma_{a:A} B(a) : \mathcal{U}_i} (\Sigma \text{ f})$$

Un élément de ce type est une paire (a, b) où $a : A$ et $b : B(a)$ (d'où le nom de paire dépendante), c'est ce que la règle suivante décrit :

$$\frac{\Gamma \vdash a : A \quad \Gamma \vdash b : B(a)}{\Gamma \vdash (a, b) : \Sigma_{a:A} B(a)} (\Sigma \text{ i})$$

Ensuite, comme les paires dépendantes sont des paires, on a de la même manière que pour les types produits les projections $\pi_1 : \Sigma_{a:A} B(a) \rightarrow A$ et $\pi_2 : \prod_{e:\Sigma_{a:A} B(a)} B(\pi_1 e)$ sur chacune des coordonnées d'un élément de $\Sigma_{a:A} B(a)$. Ces projections se comportent de manière analogue à celle des produits, ce qu'on remarque grâce aux règles d'éliminations et de calculs des Σ -types :

$$\begin{array}{cc} \frac{\Gamma \vdash e : \Sigma_{a:A} B(a)}{\Gamma \vdash \pi_1 e : A} (\Sigma_1 \text{ e}) & \frac{\Gamma \vdash e : \Sigma_{a:A} B(a)}{\Gamma \vdash \pi_2 e : B(\pi_1 e)} (\Sigma_2 \text{ e}) \\[10pt] \frac{\Gamma \vdash a : A \quad \Gamma \vdash b : B(a)}{\Gamma \vdash \pi_1 (a, b) \equiv a : A} (\Sigma_1 \equiv) & \frac{\Gamma \vdash a : A \quad \Gamma \vdash b : B(a)}{\Gamma \vdash \pi_2 (a, b) \equiv b : B(a)} (\Sigma_2 \equiv) \end{array}$$

Enfin, on a également un équivalent de la règle d'unicité des types produits pour les Σ -types :

$$\frac{\Gamma \vdash e : \Sigma_{a:A} B(a)}{\Gamma \vdash e \equiv (\pi_1 e, \pi_2 e) : \Sigma_{a:A} B(a)} (\Sigma \text{ u})$$

Exemple (Cas où B est constant). Si on considère deux types $A, B : \mathcal{U}_i$, on peut poser $C := \Sigma_{a:A} B$ qui est en tout point similaire au produit $A \times B$. En effet, si $(a, b) : C$ alors $a : A$ et $b : B(a) \equiv B$ et donc $(a, b) : A \times B$. De plus les règles étant très similaires, lorsque la famille B est constante on retrouve les règles des types produits.

1.3.6 Type vide

On introduit le type vide $\mathbf{0}$, qui ne contient aucun élément et donc n'a pas de règle d'introduction mais seulement une règle de formation et d'élimination :

$$\frac{}{\Gamma \vdash \mathbf{0} : \mathcal{U}_i} (\mathbf{0} \text{ f}) \qquad \frac{\Gamma \vdash C : \mathcal{U}_i \quad \Gamma \vdash a : \mathbf{0}}{\Gamma \vdash \text{rec}_{\mathbf{0}}(C, a) : C} (\mathbf{0} \text{ e})$$

Ainsi, on a construit une fonction $\text{rec}_{\mathbf{0}}$ de type $\prod_{C:\mathcal{U}} \mathbf{0} \rightarrow C$ qui à un type $C : \mathcal{U}_i$ associe une fonction qui ne prend aucune valeur. Par conséquent, on ne devrais jamais calculer cette fonction, c'est la raison pour laquelle il n'y a pas de règle de calcul pour ce type. La règle d'élimination agit comme le principe *ex falso quodlibet*, en effet si on construit un élément du type vide (*ie.* une preuve de \perp), alors on peut construire des éléments de n'importe quel type.

1.3.7 Type unité

Ensuite, dans l'objectif de construire tout les types finis, on commence par construire le type unité $\mathbf{1}$, contenant seulement un élément. Pour ce faire on a la règle de formation analogue à celle du type $\mathbf{0}$ avec une règle d'introduction simple car le type $\mathbf{1}$ ne possède qu'un seul élément :

$$\frac{\Gamma \text{ ctx}}{\Gamma \vdash \mathbf{1} : \mathcal{U}_i} (\mathbf{1} \text{ f}) \qquad \frac{\Gamma \text{ ctx}}{\Gamma \vdash \star : \mathbf{1}} (\mathbf{1} \text{ i})$$

La règle d'élimination de $\mathbf{1}$ permet de construire des fonctions de $\mathbf{1}$ vers un autre type C , qui sont donc des fonctions constantes et c'est ce qu'affirme la règle de calcul du type unité.

$$\frac{\Gamma \vdash C : \mathcal{U}_i \quad \Gamma \vdash c : C \quad \Gamma \vdash p : \mathbf{1}}{\Gamma \vdash \text{rec}_1(C, p, c) : C} (\mathbf{1} \text{ e})$$

$$\frac{\Gamma \vdash C : \mathcal{U}_i \quad \Gamma \vdash c : C}{\Gamma \vdash \text{rec}_1(C, \star, c) \equiv c : C} (\mathbf{1} \equiv)$$

où la fonction rec_1 est de type $\prod_{C:\mathcal{U}} \mathbf{1} \rightarrow C \rightarrow C$ (il est également possible d'intervertir les deux derniers arguments).

De plus pour ce type, on a une règle d'unicité car le seul élément de $\mathbf{1}$ est \star :

$$\frac{\Gamma \vdash p : \mathbf{1}}{\Gamma \vdash p \equiv \star : \mathbf{1}} (\mathbf{1} \text{ u})$$

1.3.8 Coproduit

Le dernier élément manquant pour construire tout les types finis sont les coproduits, qui permettent de construire un équivalent de l'union disjointe de la théorie des ensembles à partir de deux types comme l'exprime la règle de formation suivante :

$$\frac{\Gamma \vdash A : \mathcal{U}_i \quad \Gamma \vdash B : \mathcal{U}_i}{\Gamma \vdash A + B : \mathcal{U}_i} (+ \text{ f})$$

Étant donné deux types $A, B : \mathcal{U}_i$, un élément e du type $A + B$ à deux manières d'être construit :

- soit e est issu d'un élément $a : A$ et est donc de la forme $\text{inl}(a)$,
- soit e est issu d'un élément $b : B$ et est donc de la forme $\text{inr}(b)$.

On a donc deux règles d'introduction pour les coproduits :

$$\frac{\Gamma \vdash A : \mathcal{U}_i \quad \Gamma \vdash B : \mathcal{U}_i \quad \Gamma \vdash a : A}{\Gamma \vdash \text{inl}(a) : A + B} (+ \text{ inl}) \qquad \frac{\Gamma \vdash A : \mathcal{U}_i \quad \Gamma \vdash B : \mathcal{U}_i \quad \Gamma \vdash b : B}{\Gamma \vdash \text{inr}(b) : A + B} (+ \text{ inr})$$

Pour prouver des propositions sur des coproduits, une manière naturelle de faire est de raisonner par cas : ou bien on a un élément de A ou bien il s'agit d'un élément de B . Pour décrire cette méthode de raisonnement, on a la règle d'élimination des coproduits pour deux

types $A, B : \mathcal{U}_i$:

$$\frac{\Gamma \vdash C : \mathcal{U}_i \quad \Gamma, a : A \vdash g_0 a : C \quad \Gamma, b : B \vdash g_1 b : C \quad \Gamma \vdash e : A + B}{\Gamma \vdash \text{rec}_{A+B}(C, g_0, g_1, e) : C} (+ e)$$

Ainsi, la fonction rec_{A+B} est de type $\prod_{C:\mathcal{U}}(A \rightarrow C) \rightarrow (B \rightarrow C) \rightarrow A + B \rightarrow C$, et permet de faire la disjonction de cas. On a de plus deux règles décrivant le comportement de la fonction rec_{A+B} en fonction de son dernier argument :

$$\frac{\Gamma \vdash C : \mathcal{U}_i \quad \Gamma, a : A \vdash g_0 a : C \quad \Gamma, b : B \vdash g_1 b : C \quad \Gamma \vdash x : A}{\Gamma \vdash \text{rec}_{A+B}(C, g_0, g_1, \text{inl}(x)) \equiv g_0 x : C} (+ \equiv_1)$$

$$\frac{\Gamma \vdash C : \mathcal{U}_i \quad \Gamma, a : A \vdash g_0 a : C \quad \Gamma, b : B \vdash g_1 b : C \quad \Gamma \vdash y : B}{\Gamma \vdash \text{rec}_{A+B}(C, g_0, g_1, \text{inr}(y)) \equiv g_1 y : C} (+ \equiv_2)$$

Exemple (Le type **2**). Avec le coproduit et le type **1** on peut désormais construire le type **2** a deux éléments. En effet, on définit **2** par $\mathbf{2} \equiv \mathbf{1} + \mathbf{1}$, ce qui donne la règle de formation

$$\frac{\frac{\Gamma \text{ ctx}}{\Gamma \vdash \mathbf{1} : \mathcal{U}_i} \quad \frac{\Gamma \text{ ctx}}{\Gamma \vdash \mathbf{1} : \mathcal{U}_i}}{\Gamma \vdash \mathbf{1} + \mathbf{1} : \mathcal{U}_i}$$

que l'on peut résumer à :

$$\frac{\Gamma \text{ ctx}}{\Gamma \vdash \mathbf{2} : \mathcal{U}_i} (\mathbf{2} \text{ f})$$

Ensuite, comme pour le coproduit on a deux règles d'introduction :

$$\frac{\frac{\Gamma \text{ ctx}}{\Gamma \vdash \mathbf{1} : \mathcal{U}_i} \quad \frac{\Gamma \text{ ctx}}{\Gamma \vdash \mathbf{1} : \mathcal{U}_i} \quad \frac{\Gamma \text{ ctx}}{\Gamma \vdash \star : \mathbf{1}}}{\Gamma \vdash \text{inl}(\star) : \mathbf{2}} \quad \frac{\frac{\Gamma \text{ ctx}}{\Gamma \vdash \mathbf{1} : \mathcal{U}_i} \quad \frac{\Gamma \text{ ctx}}{\Gamma \vdash \mathbf{1} : \mathcal{U}_i} \quad \frac{\Gamma \text{ ctx}}{\Gamma \vdash \star : \mathbf{1}}}{\Gamma \vdash \text{inr}(\star) : \mathbf{2}}$$

En posant $0_{\mathbf{2}} \equiv \perp \equiv \text{inl}(\star)$ et $1_{\mathbf{2}} \equiv \top \equiv \text{inr}(\star)$, on peut réécrire les deux règles d'introduction plus simplement :

$$\frac{\Gamma \text{ ctx}}{\perp : \mathbf{2}} (\perp \text{ i}) \quad \frac{\Gamma \text{ ctx}}{\top : \mathbf{2}} (\top \text{ i})$$

On obtient alors la fonction $\text{rec}_{\mathbf{2}}$ de type $\prod_{C:\mathcal{U}}(\mathbf{1} \rightarrow C) \rightarrow (\mathbf{1} \rightarrow C) \rightarrow \mathbf{2} \rightarrow C$, que l'on peut également voir comme le type $\prod_{C:\mathcal{U}} C \rightarrow C \rightarrow \mathbf{2} \rightarrow C$ (car les fonctions sur **1** sont constantes) qui vérifie les règles d'élimination et de calcul suivantes :

$$\frac{\Gamma \vdash C : \mathcal{U}_i \quad \Gamma, p : \mathbf{1} \vdash g_0 p : C \quad \Gamma, p : \mathbf{1} \vdash g_1 p : C \quad \Gamma \vdash e : \mathbf{2}}{\Gamma \vdash \text{rec}_{\mathbf{2}}(C, g_0, g_1, e) : C}$$

$$\frac{\Gamma \vdash C : \mathcal{U}_i \quad \Gamma, p : \mathbf{1} \vdash g_0 p : C \quad \Gamma, p : \mathbf{1} \vdash g_1 p : C}{\Gamma \vdash \text{rec}_{\mathbf{2}}(C, g_0, g_1, \perp) \equiv g_0 \perp : C}$$

$$\frac{\Gamma \vdash C : \mathcal{U}_i \quad \Gamma, p : \mathbf{1} \vdash g_0 p : C \quad \Gamma, p : \mathbf{1} \vdash g_1 p : C}{\Gamma \vdash \text{rec}_{\mathbf{2}}(C, g_0, g_1, \top) \equiv g_0 \top : C}$$

On peut les réécrire plus simplement (et moins formellement) comme

$$\text{rec}_2(C, g_0, g_1, \perp) \equiv g_0 : C \text{ et } \text{rec}_2(C, g_0, g_1, \top) \equiv g_1 : C$$

si on identifie g_0 et g_1 à leur unique valeur respective. On remarque alors que la fonction rec_2 agit comme le "si .. alors .. sinon .." des booléens, ce qui renforce la comparaison entre le type **2** et les booléens.

Plus généralement on peut construire tout les types finis \mathbf{T}_n comme étant n fois le coproduit du type **1**, ce qui construit des types à n éléments.

1.3.9 Types inductifs : W-types

Pour construire le type des entiers \mathbf{N} , les constructeurs précédent ne suffisent pas car ils ne permettent pas de décrire le caractère inductif des entiers. Habituellement, on définit le type \mathbf{N} comme étant un élément $0 : \mathbf{N}$ et une fonction successeur $s : \mathbf{N} \rightarrow \mathbf{N}$ et un entier est de la forme 0 ou bien $s \circ s \circ \dots \circ s 0$. Une autre manière de le voir est de décrire \mathbf{N} comme un arbre dont 0 est une feuille et chacun des noeuds est d'arité un (*ie.* possède au plus un fils).

$$0 \text{ ——— } 1 \text{ ——— } 2 \text{ ——— } \dots$$

Un autre exemple de type défini de manière inductive est le type $L(A)$ des listes sur un type $A : \mathcal{U}$. La seule feuille est la liste vide notée $()$ et la fonctions jouant le rôle de constructeur inductif est la fonction $c : A \rightarrow L(A) \rightarrow L(A)$ qui a un élément $a : A$ et une liste $l : L(A)$ renvoie la liste dont le premier élément est a et le reste est l . Ainsi, toutes les listes sont de la forme $() : L(A)$ ou bien $c a_1 (c a_2 (\dots (c a_n ()))) : L(A)$.

$$\begin{array}{lcl} & (1) & \begin{array}{l} (11) \leq \dots \\ (10) \leq \dots \end{array} \\ () & \swarrow \searrow & \\ & (0) & \begin{array}{l} (01) \leq \dots \\ (00) \leq \dots \end{array} \end{array}$$

Pour généraliser les types inductifs, on introduit alors les W-types (*well-founded trees*) de Martin-Löf. Pour ce faire, on utilise un type $A : \mathcal{U}$ qui correspond aux *étiquettes* et un type $B : A \rightarrow \mathcal{U}$ qui permet de coder l'arité des noeuds : un noeud dont l'étiquette est $a : A$ aura une arité de $B(a)$. Le type résultant de ces deux types est $W_{a:A}B(a)$ que l'on construit via la règle de formation suivante :

$$\frac{\Gamma \vdash A : \mathcal{U} \quad \Gamma, a : A \vdash B(a) : \mathcal{U}}{\Gamma \vdash W_{a:A}B(a) : \mathcal{U}} \text{ (W f)}$$

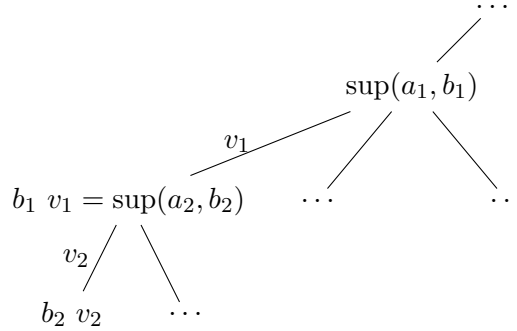
Les éléments d'un type $W_{a:A}B(a)$ sont donc des noeuds d'un arbre auxquels on associe la fonction donnant les noeuds précédents dans l'arbre. On construit ces éléments à l'aide de la règle d'introduction pour les W-types :

$$\frac{\Gamma \vdash a : A \quad \Gamma, a : A \vdash b : B(a) \rightarrow W_{x:A}B(x)}{\Gamma \vdash \text{sup}(a, b) : W_{x:A}B(x)} \text{ (W i)}$$

La fonction sup utilisé dans cette règle est donc de type

$$\text{sup} : \prod_{a:A} (B(a) \rightarrow W_{x:A}B(x)) \rightarrow W_{a:A}B(a).$$

Chaque noeud $c \equiv \text{sup}(a, b) : W_{x:A}B(x)$ est donc relié aux autres par la fonction $b : B(a) \rightarrow W_{x:A}B(x)$, en effet si on considère un élément $v : B(a)$ alors $b v$ est un prédecesseur du noeud c dans l'arbre $W_{x:A}B(x)$.



Reprenons l'exemple du type \mathbf{N} des entiers. On peut le décrire en terme de W-type en prenant $\mathbf{N} \equiv W_{x:2}B(x)$ où $B(0_2) \equiv \mathbf{0}$ et $B(1_2) \equiv \mathbf{1}$. En effet, il y a deux manières de construire un entier : ou bien c'est 0 ou bien il est de la forme $s k$ avec $k : \mathbf{N}$. Pour 0, son étiquette dans l'arbre est donc 0_2 tandis que les éléments de la forme $s k$ ont l'étiquette 1_2 . On peut donc écrire 0 avec la fonction sup :

$$0 \equiv \text{sup}(0_2, \text{rec}_{0, \mathbf{N}}).$$

De même la fonction successeur $s : \mathbf{N} \rightarrow \mathbf{N}$ peut être définie de la manière suivante :

$$s \equiv \lambda n. \text{sup}(1_2, \lambda(x : \mathbf{1}). n) : \mathbf{N} \rightarrow \mathbf{N}.$$

Et donc on a $1 \equiv s 0 \equiv \text{sup}(1_2, \lambda x. 0)$ etc.

La règle d'élimination décrit le principe d'induction sur les W-types. Pour prouver une proposition sur un type inductif, de manière analogue au principe de récurrence des entiers, on montre que la proposition est héréditaire, dans le cas présent cela revient à montrer que si la proposition est vraie sur tout les sous-arbres, alors elle est vraie sur le noeud reliant ces sous-arbres, c'est ce que dit la dernière prémisse de la règle d'élimination, qui s'énonce de la manière suivante :

$$\frac{\Gamma, a : A, b : B(a) \rightarrow W_{x:A}B(x), \quad \Gamma \vdash t : W_{x:A}B(x) \quad c : \prod_{v:B(a)} E(b v) \vdash e(a, b, c) : E(\text{sup}(a, b))}{\Gamma \vdash \text{rec}_{W_{x:A}B(x)}(E, e, t) : E(t)} \text{ (W e)}$$

La fonction e présente dans la règle est de type

$$e : \prod_{a:A} \prod_{b:(B(a) \rightarrow W_{x:A}B(x))} \left(\prod_{v:B(a)} E(b\ v) \right) \rightarrow E(\text{sup}(a, b)).$$

et pour des éléments $a : A$, $b : B(a) \rightarrow W_{x:A}B(x)$ et une preuve c de $\prod_{v:B(a)} E(b\ v)$ renvoie une preuve de $E(\text{sup}(a, b))$. La fonction $\text{rec}_{W_{x:A}B(x)}$ présente dans la conclusion de la règle précédente est une fonction qui à un prédicat (ou famille de type) E sur le type $W_{x:A}B(x)$, une fonction e comme décrit juste avant et un élément $t : W_{x:A}B(x)$ retourne une preuve (ou un élément) de $E(t)$. Ainsi, la fonction e et la fonction $\text{rec}_{W_{x:A}B(x)}$ renvoie des preuves de même nature, on peut donc imaginer une relation liant les deux : c'est la règle d'égalité (ou règle de calcul de $\text{rec}_{W_{x:A}B(x)}$).

$$\frac{\begin{array}{c} \Gamma \vdash a : A \\ \Gamma \vdash b : B(a) \rightarrow W_{x:A}B(x) \\ \Gamma, x : A, x : B(x) \rightarrow W_{x:A}B(x), z : \prod_{v:B(x)} E(y\ v) \vdash e(x, y, z) : E(\text{sup}(x, y)) \end{array}}{\Gamma \vdash \text{rec}_{W_{x:A}B(x)}(E, e, \text{sup}(a, b)) \equiv e(a, b, \lambda v. \text{rec}_{W_{x:A}B(x)}(E, e, b\ v)) : E(\text{sup}(a, b))} (W \equiv)$$

En effet, pour $a : A$ et $b : B(a) \rightarrow W_{x:A}B(x)$ la fonction $\lambda(v : B(a)). \text{rec}_{W_{x:A}B(x)}(E, e, b\ v)$ retourne une preuve (un élément) de $\prod_{v:B(a)} E(b\ v)$, ce qui correspond au dernier paramètre de la fonction e et donc le membre de droite de l'égalité est bien une preuve (un élément) de $E(\text{sup}(a, b))$ comme voulue. Les prémisses de cette règle sont de simple vérifications de typage de a , b et e .

1.3.10 Entiers naturels

Avec les W-types, nous pouvons désormais construire les entiers naturels. Pour ce faire, on note $\mathbf{N} \equiv W_{x:2}B(x)$ où $B(0_2) := \mathbf{0}$ et $B(1_2) := \mathbf{1}$. On a donc déjà vu dans le paragraphe précédent que tout élément de \mathbf{N} s'exprime sous la forme 0 ou $s\ k$ avec $k : \mathbf{N}$ et de plus on avait les expressions de 0 et de $s : \mathbf{N} \rightarrow \mathbf{N}$ suivantes :

$$\begin{cases} 0 & := \text{sup}(0_2, \text{rec}_{\mathbf{0}, \mathbf{N}}) & : \mathbf{N} \\ s & := \lambda(n : \mathbf{N}). \text{sup}(1_2, \lambda(x : \mathbf{1}). n) & : \mathbf{N} \rightarrow \mathbf{N} \end{cases}$$

On peut également réexprimer les règles de formation, d'introduction, d'élimination et d'égalité dans le cas de \mathbf{N} . Pour la règle de formation, on obtient :

$$\frac{\frac{\Gamma \vdash \mathbf{2} : \mathcal{U}}{\Gamma, a : \mathbf{2} \vdash B : \mathbf{2} \rightarrow \mathcal{U}} \quad \frac{\Gamma \vdash \mathbf{2} : \mathcal{U}}{\Gamma, a : \mathbf{2} \vdash a : \mathbf{2}}}{\Gamma, a : \mathbf{2} \vdash B(a) : \mathcal{U}} \quad \Gamma \vdash \mathbf{N} : \mathcal{U}$$

On a donc la règle simplifiée :

$$\frac{}{\Gamma \vdash \mathbf{N} : \mathcal{U}} \mathbf{N} \text{ i}$$

Ensuite, concernant la règle d'introduction on distingue deux cas puisqu'il y a deux manières de construire un élément $n : \mathbf{N}$, soit $n \equiv 0$, soit $n \equiv s \ k$ avec $k : \mathbf{N}$.

$$\frac{\frac{}{\Gamma \vdash 0_2 : \mathbf{2}} \quad \frac{\frac{}{\Gamma, 0_2 : \mathbf{2} \vdash \text{rec}_{0,\mathbf{N}} : \mathbf{0} \rightarrow \mathbf{N}}{\Gamma, 0_2 : \mathbf{2} \vdash \text{rec}_{0,\mathbf{N}} : B(0_2) \rightarrow \mathbf{N}}}{\Gamma \vdash \text{sup}(0_2, \text{rec}_{0,\mathbf{N}}) : \mathbf{N}}}{\Gamma \vdash 0 : \mathbf{N}}$$

$$\frac{\frac{}{\Gamma \vdash s : \mathbf{N} \rightarrow \mathbf{N}} \quad \Gamma \vdash k : \mathbf{N}}{\Gamma \vdash s \ k : \mathbf{N}}$$

Ce qui donne les deux règles d'introduction de \mathbf{N} :

$$\frac{}{\Gamma \vdash 0 : \mathbf{N}} (0 \text{ i}) \quad \frac{\Gamma \vdash k : \mathbf{N}}{\Gamma \vdash s \ k : \mathbf{N}} (s \text{ i})$$

Pour la règle d'élimination sur le type \mathbf{N} , on s'attend à retrouver le principe de récurrence usuel sur les entiers, à savoir que si un prédicat $E : \mathbf{N} \rightarrow \mathcal{U}$ est vrai sur 0 et que si $E(k)$ est vrai alors $E(s \ k)$ est vrai, alors $E(k)$ est vrai sur tout $k : \mathbf{N}$.

$$\frac{\Gamma \vdash k : \mathbf{N} \quad \frac{\text{Lemme 1} \quad \text{Lemme 2}}{\Gamma, a : \mathbf{2}, b : B(a) \rightarrow \mathbf{N}, c : \prod_{v:B(a)} E(b \ v) \vdash e(a, b, c) : E(\text{sup}(a, b))}}{\Gamma \vdash \text{rec}_{\mathbf{N}}(E, e, k) : E(k)}$$

Avec

$$\frac{\Gamma, a : \mathbf{1}, b : \mathbf{0} \rightarrow \mathbf{N}, c : \prod_{v:\mathbf{0}} E(b \ v) \vdash e(a, b, c) : E(\text{sup}(0_2, b))}{\Gamma, a : \mathbf{1}, b : B(\text{inl}(a)) \rightarrow \mathbf{N}, c : \prod_{v:B(\text{inl}(a))} E(b \ v) \vdash e(a, b, c) : E(\text{sup}(a, b))} \text{Lemme 1}$$

et

$$\frac{\Gamma, a : \mathbf{1}, b : \mathbf{1} \rightarrow \mathbf{N}, c : \prod_{v:\mathbf{1}} E(b \ v) \vdash e(a, b, c) : E(\text{sup}(1_2, b))}{\Gamma, a : \mathbf{1}, b : B(\text{inr}(a)) \rightarrow \mathbf{N}, c : \prod_{v:B(\text{inr}(a))} E(b \ v) \vdash e(a, b, c) : E(\text{sup}(\text{inr}(a), b))} \text{Lemme 2}$$

On peut simplifier les prémisses du Lemme 1 en remarquant que ses hypothèses sont triviales et que $\text{sup}(0_2, b) \equiv 0$ pour toute fonction $b : \mathbf{0} \rightarrow \mathbf{N}$, ce qui donne après simplification :

$$\Gamma \vdash e_0 : E(0).$$

De même, pour le Lemme 2 en remarquant qu'une fonction $b : \mathbf{1} \rightarrow \mathbf{N}$ est équivalent à choisir un $k : \mathbf{N}$ et que $c : \prod_{v:\mathbf{1}} E(b\ v)$ est similaire à $c : E(k)$, on peut réécrire la prémisse en

$$\Gamma, k : \mathbf{N}, p : E(k) \vdash e_s(k, p) : E(s\ k).$$

Finalement, on peut décomposer la fonction e du recurseur : $e_0 : E(0)$ et $e_s : \prod_{k:\mathbf{N}} E(k) \rightarrow E(s\ k)$, ce qui permet de réécrire la règle d'élimination sous la forme plus simple :

$$\frac{\Gamma \vdash k : \mathbf{N} \quad \Gamma \vdash e_0 : E(0) \quad \Gamma, k : \mathbf{N}, p : E(k) \vdash e_s(k, p) : E(s\ k)}{\Gamma \vdash \text{rec}_{\mathbf{N}}(E, e_0, e_s, k) : E(k)} \mathbf{N\ e}$$

On retrouve bien le principe de récurrence usuel, en effet pour prouver un prédicat sur les entiers \mathbf{N} il suffit de le prouver sur 0 puis qu'il est héréditaire *ie.* s'il est vérifié sur un entier $k : \mathbf{N}$ alors il est vérifié sur $s\ k$ l'entier suivant.

1.3.11 Listes

Un autre exemple de type inductif est le type des listes sur un type $A : \mathcal{U}_i$, que l'on note $L(A)$. Pour la construire on utilise alors le W-type $W_{x:\mathbf{1}+A} B(x)$ où $B(\text{inl}(\star)) \equiv \mathbf{0}$ et $B(\text{inr}(a)) \equiv \mathbf{1}$, autrement dit on pose

$$L(A) \equiv W_{x:\mathbf{1}+A} \text{rec}_{\mathbf{1}+A}(\mathcal{U}_i, \lambda(x : \mathbf{1}). \mathbf{0}, \lambda(a : A). \mathbf{1}, x).$$

De là, on déduit la règle de formation de $L(A)$:

$$\frac{\frac{\Gamma \text{ ctx}}{\Gamma \vdash A : \mathcal{U}_i} \quad \frac{\Gamma \vdash \mathbf{1} : \mathcal{U}_i}{\Gamma \vdash \mathbf{1} + A : \mathcal{U}_i} \quad \frac{\Gamma, x : \mathbf{1} + A \vdash \text{rec}_{\mathbf{1}+A}(\mathcal{U}_i, \lambda(y : \mathbf{1}). \mathbf{0}, \lambda(y : A). \mathbf{1}, x) : \mathcal{U}_i}{\Gamma, x : \mathbf{1} + A \vdash B(x) : \mathcal{U}_i}}{\Gamma \vdash L(A) : \mathcal{U}_i}$$

Plus simplement,

$$\frac{\Gamma \vdash A : \mathcal{U}_i}{\Gamma \vdash L(A) : \mathcal{U}_i} L\ f$$

Ensuite pour construire un élément on a deux constructeurs :

- La liste vide, notée $()$ que l'on définit comme $() \equiv \text{sup}(\text{inl}(\star), \text{rec}_{\mathbf{0}}(L(A))) : L(A)$,
- L'ajout d'un élément en tête de liste via la fonction $c : A \rightarrow L(A) \rightarrow L(A)$ qui est défini de la manière suivante :

$$c \equiv \lambda(a : A). \lambda(l : L(A)). \text{sup}(a, \lambda(x : \mathbf{1}). l).$$

que l'on peut également noter $::$ de manière infixé.

Ainsi, une liste $l \equiv (a_1, \dots, a_k) : L(A)$ est définie par

$$l \equiv c\ a_1\ (a_2, \dots, a_k) \equiv a_1 :: (a_2, \dots, a_k) \equiv \text{sup}(a_1, \lambda(x : \mathbf{1}). (a_2, \dots, a_k)).$$

On remarque alors une structure d'arbre dans le type des listes, dont la racine est $()$ et la fonction donnant les successeurs d'un noeud l est la fonction $\lambda(a : A). c a l : A \rightarrow L(A)$.

On a donc deux règles d'introduction correspondant à ces deux cas.

$$\begin{array}{c}
 \frac{\frac{\Gamma \vdash \mathbf{1} : \mathcal{U}_i \quad \Gamma \vdash A : \mathcal{U}_i \quad \Gamma \vdash \star : \mathbf{1}}{\Gamma \vdash \text{inl}(\star) : \mathbf{1} + A} \quad \frac{\Gamma \vdash \text{rec}_{\mathbf{0}}(L(A)) : \mathbf{0} \rightarrow L(A)}{\Gamma \vdash \text{rec}_{\mathbf{0}}(L(A)) : B(\text{inl}(\star)) \rightarrow L(A)} \\
 \hline
 \Gamma \vdash \text{sup}(\text{inl}(\star), \text{rec}_{\mathbf{0}}(L(A))) : L(A) \\
 \hline
 \Gamma \vdash () : L(A)
 \end{array}$$

$$\begin{array}{c}
 \frac{\Gamma \vdash l : L(A)}{\Gamma, x : \mathbf{1} \vdash l : L(A)} \\
 \hline
 \Gamma \vdash \lambda(x : \mathbf{1}). l : \mathbf{1} \rightarrow L(A) \\
 \hline
 \frac{\Gamma \vdash \mathbf{1} : \mathcal{U}_i \quad \Gamma \vdash A : \mathcal{U}_i \quad \Gamma \vdash a : A \quad \Gamma \vdash \lambda(x : \mathbf{1}). l : \text{rec}_{\mathbf{1}+A}(\mathcal{U}_i, \mathbf{0}, \mathbf{1}, \text{inr}(a)) \rightarrow L(A)}{\Gamma \vdash \text{inr}(a) : \mathbf{1} + A \quad \Gamma \vdash \lambda(x : \mathbf{1}). l : B(\text{inr}(a)) \rightarrow L(A)} \\
 \hline
 \Gamma \vdash \text{sup}(\text{inr}(a), \lambda(x : \mathbf{1}). l) : L(A) \\
 \hline
 \Gamma \vdash a :: l : L(A)
 \end{array}$$

Plus simplement,

$$\frac{\Gamma \vdash A : \mathcal{U}_i}{\Gamma \vdash () : L(A)} () \text{ i} \quad \frac{\Gamma \vdash A : \mathcal{U}_i \quad \Gamma \vdash a : A \quad \Gamma \vdash l : L(A)}{\Gamma \vdash a :: l : L(A)} c \text{ i}$$

A partir de la règle d'élimination des W-types, on peut déduire la règle d'élimination du type $L(A)$:

$$\begin{array}{c}
 \text{Lemme 1} \quad \text{Lemme 2} \\
 \hline
 \Gamma \vdash l : L(A) \quad \Gamma, a : \mathbf{1} + A, b : B(a) \rightarrow L(A), c : \prod_{v:B(a)} E(b \ v) \vdash e(a, b, c) : E(\text{sup}(a, b)) \\
 \hline
 \Gamma \vdash \text{rec}_{L(A)}(E, e, l) : E(l)
 \end{array}$$

$$\frac{\Gamma, a : \mathbf{1}, b : \mathbf{0} \rightarrow L(A), c : \prod_{v:\mathbf{0}} E(b \ v) \vdash e(a, b, c) : E(())}{\Gamma, a : \mathbf{1}, b : B(\text{inl}(a)) \rightarrow L(A), c : \prod_{v:B(\text{inl}(a))} E(b \ v) \vdash e(a, b, c) : E(\text{sup}(\text{inl}(a), b))} \text{Lemme 1}$$

$$\frac{\Gamma, a : A, b : \mathbf{1} \rightarrow L(A), c : \prod_{v:\mathbf{1}} E(b \ v) \vdash e(a, b, c) : E(a :: b)}{\Gamma, a : A, b : B(\text{inr}(a)) \rightarrow L(A), c : \prod_{v:B(\text{inr}(a))} E(b \ v) \vdash e(a, b, c) : E(\text{sup}(\text{inr}(a), b))} \text{Lemme 2}$$

Le lemme 1 correspond à une preuve de E sur la liste vide $()$ dont les hypothèses sont triviales.

On peut donc réécrire sa prémisse sous une forme plus simple

$$\Gamma \vdash e_0 : E(()).$$

De même, on peut simplifier le lemme 2 en remarquant que $b : \mathbf{1} \rightarrow L(A)$ est équivalent à une liste $l \equiv b \star$, et que $c : \prod_{v:\mathbf{1}} E(b \ v)$ est une preuve de $E(l)$:

$$\Gamma, a : A, l : L(A), p : E(l) \vdash e_s(a, l, p) : E(a :: l).$$

On peut aussi réécrire e en le décomposant en $e_0 : E(())$ et $e_s : \prod_{a:A} \prod_{l:L(A)} E(l)$ pour correspondre à ces deux cas, ce qui donne finalement la règle

$$\frac{\Gamma \vdash l : L(A) \quad \Gamma \vdash e_0 : E(()) \quad \Gamma, a : A, l : L(A), p : E(l) \vdash e_s(a, l, p) : E(a :: l)}{\Gamma \vdash \text{rec}_{L(A)}(E, e_0, e_s, l) : E(l)} L \ e$$

Ce qui correspond à la preuve par induction sur les listes, à savoir que si un prédicat E sur $L(A)$ est vraie sur la liste vide $()$ et qu'il est héréditaire *ie.* si E est vraie sur une liste l et si $a : A$ alors E est vérifié sur $a :: l$, alors E est vérifié sur toute les listes.

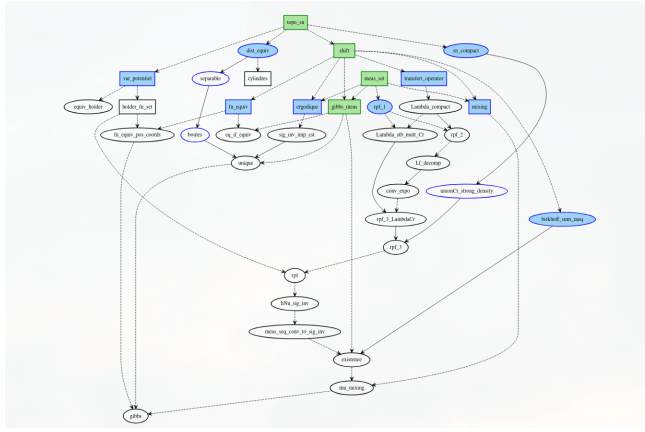
1.4 Correspondance de Curry-Howard

2 Formalisation du théorème de Bowen en Lean

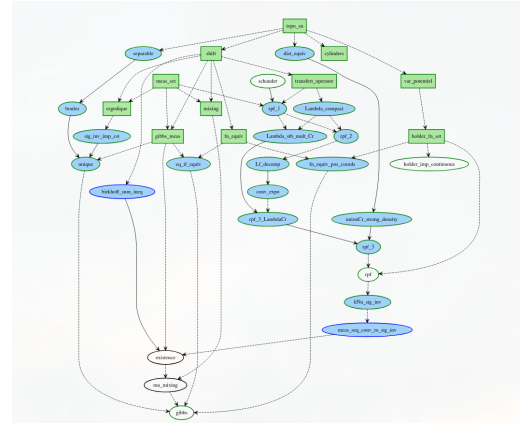
Cette section est un retour d'expérience sur l'utilisation de Lean en tant qu'outil de formalisation pour les mathématiques.

Durant ce TER, j'ai donc utilisé Lean pour formaliser le théorème de Bowen, dont une preuve figure dans mon rapport de stage en annexe (preuve initialement due à R. Bowen). Ce théorème établit l'existence et l'unicité d'une certaine mesure de probabilité dite de Gibbs sur un espace métrique particulier, et donc ce théorème fait intervenir notamment de la topologie et de la théorie de la mesure.

Pour formaliser ce théorème, j'ai donc eu recours à des outils extérieurs à Lean comme `leanblueprint` (AJOUTER LIEN) qui permet à partir d'un texte mathématiques d'obtenir un graphe décrivant les liens entre les différents lemmes, théorèmes et définitions intermédiaires et d'en donner l'état d'avancement dans le code Lean associé.



(a) État initial du graphe



(b) État final du graphe

Les cases rectangulaires sont les définitions, les ellipses sont les lemmes, théorèmes, corollaires et propositions. Les couleurs en fond indiquent l'état d'avancement des preuves : le vert foncé pour les lemmes prouvés et dont les parents sont également prouvés, le vert clair pour les lemmes prouvés et le bleu pour les lemmes prêt à être prouvés (*ie.* toutes les définitions nécessaires sont formalisées). Enfin les couleurs des bordures indiquent l'état d'avancement des énoncés des lemmes et des définitions : le vert pour les cases dont l'énoncé est formalisé et le bleu pour les cases dont l'énoncé n'est pas formalisé mais prêt à l'être.

2.1 Formalisation de l'énoncé du théorème

Dans un premier temps, j'ai donc converti chaque définition et résultat nécessaire pour le théorème de Bowen en code Lean afin de pouvoir écrire l'énoncé du théorème. Pour ce faire on a besoin notamment de définir la notion de mesure de Gibbs puis on peut alors énoncé le théorème avec le code suivant :

```
class IsGibbs (φ : Bernoulli Z n → ℝ) (μ : Measure (Bernoulli Z n)) extends InvariantProb μ where
  gibbs_prop : ∃ P : ℝ, ∃ c₁ c₂ : ENNReal, c₁ > 0 ∧ c₂ > 0 ∧ ∀ x : Bernoulli Z n, ∀ m : ℕ,
    μ (cylinder x m) / nnexp (- P * m + ∑ k ∈ Ico 0 m, φ (shift^[k] x)) ∈ Icc (c₁ : ENNReal) (c₂ : ENNReal)

theorem gibbs (φ : Bernoulli Z n → ℝ) [HolderLike φ] :
  ∃! μ : Measure (Bernoulli Z n), IsGibbs φ μ := by
```

Cependant, la preuve de ce résultat nécessite un certain nombre de lemmes intermédiaires qu'il faut également prouver et donc la preuve du théorème était trop longue par rapport au temps imparti.

On a donc décidé de se concentrer sur la formalisation des énoncés et sur la preuve d'un lemme important de topologie des espaces ultramétriques, pour expérimenter tout les aspects d'un assistant de preuves.

Pour la formalisation des énoncés il a donc fallu dans un premier temps adapter le rapport de stage au format demandé par l'outil lean-blueprint, en ajoutant des détails et en décomposant certains énoncés pour correspondre davantage à la structure du code Lean. L'étape suivante était de traduire chaque définition et lemmes (sans les preuves) en un code le plus clair possible pour faciliter le travail d'écriture des preuves suivant l'ordre préconisé par le graphe de dépendance. Enfin, j'ai pu commencer à écrire des morceaux de preuves pour les lemmes les plus simples. Finalement au vu du nombre de preuve à convertir en code, il a fallu choisir un résultat dont la preuve était moins conséquente pour s'y consacrer.

2.2 Preuve d'un résultat topologique

Le choix qui a été fait était de prouver un théorème de topologie permettant de décomposer les ouverts d'un espace ultramétriques compact en une union disjointe de boules. Ce résultat était nécessaire pour réécrire la mesure des ouverts en somme de mesure de boules pour lesquelles on possède une estimation dans le cas des mesures de Gibbs.

Afin de prouver ce résultat, la première étape était de réécrire de manière la plus détaillé possible sa preuve et d'en donner les étapes intermédiaires pour ensuite les convertir en lemme dans Lean pour pouvoir écrire les preuves de ces lemmes. L'étape finale à donc été d'écrire la preuve du théorème en utilisant tout les lemmes précédents.

Cependant la traduction des preuves en Lean ne se fait pas littéralement, il faut souvent adapter les énoncés pour les faire correspondre aux lemmes déjà existants et prouvés dans Mathlib (la bibliothèque de Lean contenant une large variété de théorèmes). Ainsi, nous avons donc transformés l'énoncé mathématique standard, à savoir

Théorème. *Soit \mathcal{O} un ouvert borné de E , alors il existe une partie $R \subseteq \mathcal{O}$ et une fonction $r : R \rightarrow \mathbf{R}_+^*$ telle que*

$$\mathcal{O} = \bigsqcup_{x \in R} B(x, r(x)).$$

en l'énoncé suivant, utilisant à la fois la théorie des types et des propriétés déjà présentes dans Mathlib :

Théorème. *Soit \mathcal{O} un ouvert borné de E . Alors on a les propriétés suivantes :*

1. $\bigcup_{s:S} \Phi(s) = \mathcal{O}$
2. Si $s_1, s_2 : S$ sont distincts alors $\Phi(s_1) \cap \Phi(s_2) = \emptyset$.

où S est un type et $\Phi : S \rightarrow B$ une fonction construites à partir de \mathcal{O} et B est le type des boules de E incluses dans \mathcal{O} .

On peut alors remarquer que les deux énoncés sont en fait équivalents, il s'agit simplement d'une reformulation plus maniable en Lean d'un même théorème, car elle fait intervenir des types et des fonctions largement utilisées dans Mathlib et qui sont donc plus faciles d'utilisation. Une fois converti en Lean, il peut s'écrire avec le code suivant :

```
theorem partition (hO : IsOpen O) (O_bdd : ∃ (x : X), ∃ r > 0, O ⊆ ball x r) :  
  let Φ := iBall (Obdd O_bdd)  
  ∪ s, Φ s = O ∧ Pairwise (onFun Disjoint (fun s => (Φ s).1)) := by
```

Une preuve de ce théorème se trouve dans la section suivante et une formalisation de ce théorème est disponible ici (AJOUTER LIEN).

3 Topologie des espaces ultramétriques

Pour montrer l'unicité dans le théorème de Bowen, on a besoin d'un résultat de topologie de certains espaces, appelés espaces ultramétriques, qui sont des espaces métriques où l'inégalité triangulaire habituelle est remplacée par une inégalité dite ultramétrique :

$$\forall x, y, z \in E, d(x, z) \leq \max(d(x, y), d(y, z)).$$

Cette inégalité donne de nombreux résultats topologiques très différents des espaces métriques, notamment sur les triangles et les boules.

Le théorème permettant de prouver l'unicité du théorème de Bowen est le suivant, et nous allons en donner une preuve dans cette section, puis une formalisation possible en Lean.

Théorème 3.1. *Soit (E, d) un espace ultramétrique et \mathcal{O} un ouvert borné de E , alors il existe une partie $R \subseteq \mathcal{O}$ et une application $r: R \rightarrow \mathbf{R}_+^*$ tels que*

$$\mathcal{O} = \bigsqcup_{x \in R} B(x, r(x)).$$

De plus, si E est séparable alors on peut imposer que R soit au plus dénombrable.

Dans la suite on fixe (E, d) un espace ultramétrique. Commençons par quelques lemmes décrivant les relations entre les boules dans ces espaces.

Lemme 3.2. *Soit $x, y \in E$ et un réel $r > 0$, si $y \in B(x, r)$, alors $B(x, r) = B(y, r)$*

Démonstration. Supposons que $y \in B(x, r)$. Soit $z \in B(x, r)$, alors

$$d(y, z) \leq \max(d(y, x), d(x, z)) \leq \max(r, r) \leq r,$$

car $y, z \in B(x, r)$. Donc on a une inclusion : $B(x, r) \subseteq B(y, r)$.

Réciproquement comme $y \in B(x, r)$ on a $x \in B(y, r)$ par symétrie de la distance et donc avec le même raisonnement on a l'autre inclusion. Finalement, $B(x, r) = B(y, r)$. \square

Lemme 3.3. *Soit $x, y \in E$ et deux réels $r, s > 0$, alors il y a trois possibilités :*

1. $B(x, r) \subseteq B(y, s)$,
2. $B(y, s) \subseteq B(x, r)$,
3. $B(x, r) \cap B(y, s) = \emptyset$.

Démonstration. Supposons que $B(x, r) \cap B(y, s) \neq \emptyset$, alors soit $z \in B(x, r) \cap B(y, s)$. On peut alors écrire $B(x, r) = B(z, r)$ et $B(y, s) = B(z, s)$ grâce au lemme 3.2, et ainsi on a bien le résultat voulu en fonction de l'ordre de r et s . \square

Lemme 3.4. *Soit $(x_i)_{i \in I}$ une famille de point de E et $(r_i)_{i \in I}$ une famille de réels strictement positifs. De plus, supposons qu'il existe $x \in E$ tel que $x \in B(x_i, r_i)$ pour tout $i \in I$ et que $R = \sup_{i \in I} r_i < \infty$. Alors*

$$\bigcup_{i \in I} B(x_i, r_i) = B(x, R).$$

Démonstration. Commençons par réécrire chaque boule en changeant son centre grâce au lemme 3.2 et notons $R = \sup_{i \in I} r_i < \infty$, on a alors l'inclusion

$$\bigcup_{i \in I} B(x_i, r_i) = \bigcup_{i \in I} B(z, r_i) \subseteq B(z, R).$$

Réciproquement si $y \in B(z, R)$, alors il existe $i_0 \in I$ tel que $d(y, z) \leq r_{i_0} \leq R$ et donc $y \in B(z, r_{i_0}) \subseteq \bigcup_{i \in I} B(z, r_i)$. Finalement, l'union de ces boules est encore une boule. \square

On notera dans la suite $\mathcal{O} \subseteq E$ un ouvert borné, et donc on a pour chaque $x \in \mathcal{O}$ un réel $r_x > 0$ tel que $B(x, r_x) \subseteq \mathcal{O}$. On a alors

$$\mathcal{O} = \bigcup_{x \in \mathcal{O}} B(x, r_x).$$

Remarque. On peut voir les $(r_x)_{x \in \mathcal{O}}$ comme une application $r: \mathcal{O} \rightarrow \mathbf{R}_+^*$.

Definition 3.1. On note $B(\mathcal{O})$ l'ensemble des boules incluses dans \mathcal{O} , en particulier :

$$B(\mathcal{O}) := \{B(x, r) \mid x \in \mathcal{O} \wedge r > 0 \wedge B(x, r) \subseteq \mathcal{O}\} \subseteq \mathcal{P}(E).$$

Soit $\mathcal{U} \subseteq B(\mathcal{O})$, on définit une relation $\sim_{\mathcal{U}}$ (ou plus simplement \sim s'il n'y a pas d'ambiguïté) sur \mathcal{U} par :

$$\forall u, v \in \mathcal{U}, \quad u \sim_{\mathcal{U}} v \iff \exists w \in \mathcal{U}, u \cup v \subseteq w.$$

Proposition 3.5. Pour tout $\mathcal{U} \subseteq B(\mathcal{O})$, la relation $\sim_{\mathcal{U}}$ est une relation d'équivalence.

Démonstration. Soit $u_1, u_2, u_3 \in \mathcal{U}$ trois boules.

Pour la réflexivité, on considère $w = u_1 \in \mathcal{U}$ et on a bien $u_1 \sim u_1$.

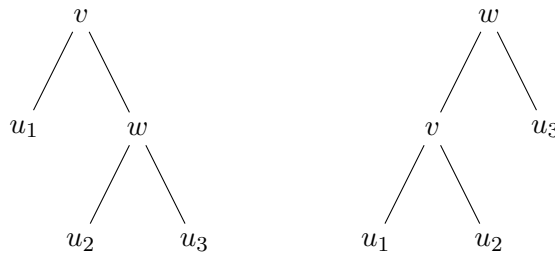
Pour la symétrie, la définition de la relation est clairement symétrique.

Enfin pour la transitivité, on suppose que $u_1 \sim u_2$ et $u_2 \sim u_3$. On a alors $v, w \in \mathcal{U}$ tels que

$$u_1 \subseteq v, u_2 \subseteq v, u_2 \subseteq w \text{ et } u_3 \subseteq w.$$

Ainsi, $\emptyset \neq u_2 \subseteq v \cap w$, or v et w sont des boules d'un espace ultramétrique. On a alors deux cas :

- $v \subseteq w$ dans ce cas on a $u_1 \overset{v}{\sim} u_3$
- $w \subseteq v$ et alors on a $u_1 \overset{w}{\sim} u_3$



Donc $\sim_{\mathcal{U}}$ est bien une relation d'équivalence sur \mathcal{U} . \square

Pour la suite de la section on fixe $\mathcal{U} \subseteq B(\mathcal{O})$ un sous-ensemble de l'ensemble des boules incluses dans \mathcal{O} .

Definition 3.2. Soit $u \in \mathcal{U}$, la classe d'équivalence de u pour la relation \sim est noté \bar{u} . On introduit également $\mathcal{B}_u \in B(\mathcal{O})$ l'union des éléments de la classe d'équivalence de u :

$$\mathcal{B}_u := \bigcup_{u \sim u'} u' \subseteq \mathcal{O}.$$

Remarquons que \mathcal{B}_u est une boule dès lors que cette union est bornée (d'après le lemme 3.4), or cette $\mathcal{B}_u \subseteq \mathcal{O}$ et \mathcal{O} est borné donc \mathcal{B}_u est toujours une boule.

Definition 3.3. Soit R un système complet de représentant pour la relation \sim . On pose alors

$$\mathcal{U}' := \mathcal{U} \cup \{\mathcal{B}_u \mid u \in R\} \subseteq B(\mathcal{O}).$$

car $\mathcal{B}_u \in B(\mathcal{O})$ pour chaque $u \in R$.

On considère désormais $\sim' = \sim_{\mathcal{U}'}$ qui est encore une relation d'équivalence, et soit R' un système complet de représentant pour la relation \sim' .

Théorème 3.6. Soit \mathcal{O} un ouvert borné de E . Avec les notations introduites précédemment on a

$$\mathcal{O} = \bigsqcup_{u \in R'} \mathcal{B}_u.$$

Démonstration. On commence par montrer que cette union est bien égale à \mathcal{O} . En considérant $\mathcal{U} = \{B(x, r_x) \mid x \in \mathcal{O}\}$,

$$\mathcal{O} = \bigcup_{u \in \mathcal{U}} u = \bigcup_{u \in \mathcal{U}'} u = \bigcup_{u \in R'} \left(\bigcup_{v \sim' u} v \right) = \bigcup_{u \in R'} \mathcal{B}_u$$

Il reste encore à montrer que cette union est disjointe. Supposons que $\mathcal{B}_u \cap \mathcal{B}_v \neq \emptyset$. Alors on a $\mathcal{B}_u \subseteq \mathcal{B}_v$ ou $\mathcal{B}_v \subseteq \mathcal{B}_u$ par le lemme 3.3. Dans les deux cas on a $u \sim' v$ avec $w = \mathcal{B}_v \in \mathcal{U}'$ dans le premier cas et $w = \mathcal{B}_u \in \mathcal{U}'$ dans le second. Or R est un système complet de représentant pour \sim' et donc nécessairement $u = v$. Finalement les $(\mathcal{B}_u)_{u \in R'}$ sont deux à deux disjoints et leur union est égale à \mathcal{O} , ce qui conclut la preuve du théorème 3.1. \square

Avec la même preuve on obtient en changeant une hypothèse la même conclusion.

Corollaire 3.6.1. Soit E un espace ultramétrique tel qu'il existe $(x_i)_{i \in I} \in E^I$ et $(r_i)_{i \in I}$ des réels strictement positifs vérifiant la propriété suivante :

$$E = \bigcup_{i \in I} B(x_i, r_i) \quad \text{et} \quad \sup_{i \in I} r_i < \infty.$$

Alors pour tout ouvert \mathcal{O} de E , il existe $R \subseteq E$ et $r : R \rightarrow \mathbf{R}_+^*$ tel que

$$\mathcal{O} = \bigsqcup_{x \in R} B(x, r(x)).$$

Démonstration. On réécrit \mathcal{O} comme l'union suivante :

$$\mathcal{O} = \bigsqcup_{i \in I} B(x_i, r_i) \cap \mathcal{O}.$$

Cette union est disjointe car les boules des espaces ultramétriques sont disjointe ou bien incluses l'une dans l'autre, donc on peut se ramener à ce cas (A VÉRIFIER). Ainsi, pour tout $i \in I$, $B(x_i, r_i) \cap \mathcal{O}$ est un ouvert borné et donc peut être écrit comme une union disjointe de boule. De cette manière on obtient le résultat voulu. \square