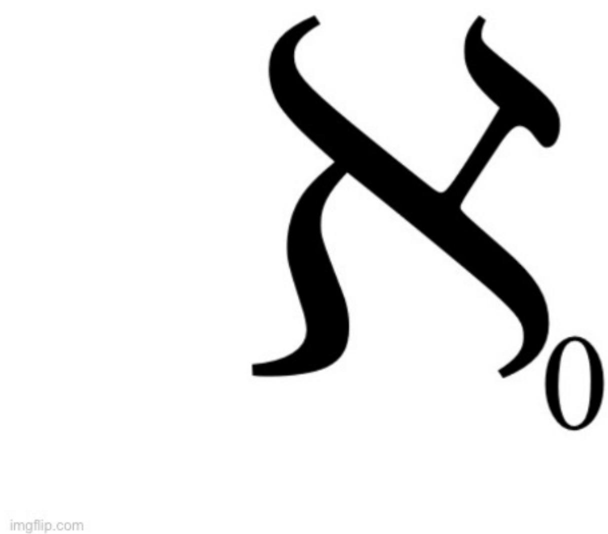
Projet de recherche:
Une preuve de l'indépendance de l'hypothèse du continu, par Dana Scott

Nathan Boudol
L3 Maths - Info

Mai 2024



Contents

1 Introduction **3**

2 Preuve : Indépendance de l'hypothèse du continu **3**

2.1 Formulation de l'hypothèse du continu 3

2.2 Axiomatique sur une théorie de plus grand ordre des nombres réels; formulation finale de (CH) 4

2.3 Construction d'un modèle 6

2.3.1 Les réels aléatoires 6

2.3.2 Concept de fonctions aléatoires et fonctionnelles 11

2.3.3 Preuve de la validité de l'axiome du choix (AC) dans le modèle 13

2.4 La négation de l'hypothèse du continu dans un modèle approprié 16

1 Introduction

Le travail s'appuie sur la preuve de Dana Scott, publié en juin 1967

L'indépendance de l'hypothèse du continu est l'un des grands problèmes de la théorie des ensembles depuis que Cantor l'a posé à la fin du 19*ème* siècle, étant même le premier problème énoncé dans les *Problèmes de Hilbert*. Ce n'est qu'en 1940 avec Gödel et 1963 avec Cohen, au travers de méthodes tel que celle du forcing, qu'ils montrèrent que l'hypothèse du continu était indépendante des axiomes ZFC (i.e. indécidable dans ZFC).

Contrairement à Cohen, Scott ne se contente que de concepts les plus minimaux possibles, dans le sens où il se limite dans les notions utilisées. C'est donc une approche différente que nous a proprosée Scott, notamment avec l'utilisation de modèles non standards. Ils ont tous les trois apportés de nouvelles perspectives dans le développement de la théorie des ensembles et de la logique mathématique au travers de leurs travaux.

2 Preuve : Indépendance de l'hypothèse du continu

2.1 Formulation de l'hypothèse du continu

Scott va, moyennant le moins de notions mathématiques possible, formuler cette hypothèse avec des symboles logiques. L'hypothèse de départ est la suivante :

$$(CH) \quad 2^{\aleph_0} = \aleph_1$$

Il nous dit, par ailleurs, que la référence a des $\aleph$ peut être facilement éviter. En effet, avec l'axiome du choix, chaque cardinal est un $\aleph$. Par conséquent, l'hypothèse du continu nous stipule qu'il n'y a pas de cardinal strcitement compris entre $\aleph_0$ et $2^{\aleph_0} = \aleph_1$.

Ensuite, Scott nous dit que l'ensemble le plus naturel avec un tel cardinal $\aleph_1$ est l'ensemble des nombres réels. Par conséquent, (CH) peut encore être reformulée par : *Chaque ensemble de nombres réels est soit dénombrable ou de même cardinal que* $\mathbb{R}$.

Munissons nous seulement de quelques objets mathématiques (que Scott juge "*familiers*") : les entiers, les réels, des sous-ensembles arbitraires de réels ainsi que des fonctions sur les réels. Formalisons cela avec des symboles logiques.

Notons x, y des réels, X un ensemble de réels et f, g des fonctions sur les réels. $\mathbb{N}$ comme a son habitude désigne les entiers. Nous pouvons alors écrire :

$$(CH') \quad \forall X[\exists f \forall y \in X \exists x \in N[y = f(x)] \vee \exists g \forall y \exists x \in X[y = g(x)]]$$

à lire comme : il existe une surjection de mon ensemble sur $\mathbb{N}$ **ou** sur $\mathbb{R}$.

Dans un souci d'économie de concepts mathématiques, Scott va remplacer les $\forall y \in X$ par $\forall y[X(y) = 0]$, une fonction indicatrice de l'ensemble. L'intérêt de cela sera dans le système axiomatique choisi, qui sera par conséquent plus minimal étant donné que nous nous abstenons de définir ce qu'est un ensemble.

2.2 Axiomatique sur une théorie de plus grand ordre des nombres réels; formulation finale de (CH)

Pour le moment, seuls les notions de réels et fonctions de réels ont été mentionné. Les formules utilisant ces objets (à l'aide des quantificateurs, connecteurs logiques habituels,..) sont certainement suffisant pour formuler (CH), mais Scott nous dit qu'il y a beaucoup d'objets qui ne peuvent pas être définis avec autant de restrictions sur les termes utilisés.

PPour cela, il se base sur des exemples de fonctionnelles (fonctions sur les fonctions), de fonctions sur les fonctionnelles, etc. Le fait qu'il n'y ait pas mention de ceux-ci dans (CH) ne signifie pas nécessairement qu'ils ne sont pas nécessaires pour fournir une preuve de cette hypothèse. Pour étayer son propos, il cite le théorème d'incomplétude de Gödel qui stipule que les objets servant à la preuve d'un énoncé peuvent se situer à un degrès supérieur du modèle actuel.

Cependant, concernant l'hypothèse du continu, Cohen a prouvé que (CH) était indémontrable, peu importe le niveau considéré, dans le système axiomatique de Zermelo-Fraenkel muni de l'axiome du choix (et donc son indépendance à la théorie des ensembles).

Pour pouvoir axiomatiser sa théorie, Scott utilise dans un premier temps les notations ordinaires (donc sur les réels) :
- x, y, z les variables
- 0, 1, +, ., $\leq$ et =
- fonctions sur les réels : f, g, h (avec la notation f(x))
- fonctionnelles : F, G (avec la notation F(f), G(f))

Une **formule atomique** est alors une équation ou inéquation ne contenant que ces notations là; et une **formule** est le résultat de l'application de connecteurs logiques $(\wedge, \vee, \rightarrow, \leftrightarrow)$ sur des formules atomiques. Par la suite, les lettres majuscules A, B désigneront des formules auxquelles nous pouvons attacher des quantificateurs $(\forall, \exists)$. Il est à noter qu'une variable sans quantificateur est dite "*libre*", et est "*liée*" sinon. Des variables libres peuvent être substituer afin d'être plus précis et moins ambigü. Enfin, une formule est dite "*vraie*" ou "*valide*" si elle est prouvable dans le système axiomatique dans lequel nous nous situons.

Voici les axiomes que Scott a décidé de se munir pour la preuve :

Un premier groupe, ceux de la logique propositionnelle :

$$
\begin{array}{ll}
(PL) & A \to [B \to A] \\
& A \to [B \to C] \to [[A \to B] \to [A \to C]] \\
& [\neg B \to \neg A] \to [A \to B]] \\
& A \wedge B \to A \\
& A \wedge B \to B \\
& A \to [B \to [A \wedge B]] \\
& A \to [A \vee B]] \\
& B \to [A \vee B]] \\
& [A \to C] \to [[B \to C] \to [[A \wedge B] \to C] \\
& [A \leftrightarrow B] \to [A \to B] \\
& [A \leftrightarrow B] \to [A \to B] \\
& [A \to B] \to [[B \to A] \to [A \leftrightarrow B]]
\end{array}
$$

Ensuite, ceux concernant les quantificateurs :

$$
\begin{array}{ll}
(QL) & \forall v \; A(v) \to A(t) \\
& A(v) \to \exists t \; A(t)
\end{array}
$$

L'égalité :

$$
\begin{array}{ll}
(EL) & t = t \\
& u = t \to A(t) = A(u)
\end{array}
$$

où u,t peuvent être des réels, fonctions ou fonctionnelles. Scott fait ensuite allusion au fait que ce schéma d'axiomes est commun à toutes les théories, tout comme l'inférence (dans le cadre de la logique) avec les règles du $\exists, \forall et \to$.

Pour continuer, en sortant du domaine de la logique, nous pouvons parler d'ordre. Il introduit alors un ordre *complet*, sous la forme suivante :

$$\exists y \forall x [f(x) \leq y] \to \exists z \forall y [z \leq y \leftrightarrow \forall x [f(x) \leq y]]$$

qui traduit le fait qu'une fonction bornée possède une plus petite borne supérieur (il juge que c'est le plus simple pour son système).

Mais cette formule implique une varibale de type fonction, et il n'y a pas d'axiomes les concernant. En voici donc :

$$(EF) \quad f = g \leftrightarrow \forall x[f(x) = g(x)]$$
$$F = G \leftrightarrow \forall f[F(f) = G(f)]$$

$$(AC) \quad \forall x\,\exists y\,A(x,y) \rightarrow \exists f\,\forall x\,A(x,f(x))$$
$$\forall f\,\exists y\,B(f,y) \rightarrow \exists F\,\forall f\,B(f,F(f))$$

qui traduisent l'égalité pour les fonctions et fonctionnelles; ainsi qu'à l'axiome du choix sur les réels et les fonctions. Enfin, Scott nuance sa définition de fonctions, en disant que si nous voulons utiliser des fonctions avec plusieurs arguments, il suffit de définir pour un couple (x, y) donné :

$$f(z) = x\ si\ z = 0\ /\ y\ si\ z = 1\ /\ 0\ sinon$$

Nous avons alors une fonctionnelle, qui permet justement les fonctions à plusieurs arguments. Cela évite une éventuelle règle supplémentaire, même si cela reste possible.

Finalement, il ne manque plus qu'à définir la notion "*être un entier*", qui correspond à l'ensemble dénombrable infini usuel. Si y est un entier, alors :

$$N(y) \leftrightarrow \forall f[f(0) = 0] \wedge \forall x[0 \leq x \rightarrow f(x) = f(x+1)] \rightarrow f(y) = 0]$$

Il faut lire que $\mathbb{N}$ est un ensemble qui contient 0, ainsi que tous ses successeurs (positifs donc). En remplaçant cette définition dans notre ancienne formule (CH'), nous obtenons au final :

$$(CH'') \quad \forall h\,[\exists f \forall y[h(y) = 0 \rightarrow \exists x[N(x) \wedge y = f(x)]] \vee \exists g \forall y \exists x[h(x) = 0 \wedge y = g(x)]]$$

2.3 Construction d'un modèle

2.3.1 Les réels aléatoires

L'idée principale des deux parties suivantes est de remarquer que ce qui est vrai sur les réels ordinaires l'est aussi (presque totalement) sur les réels aléatoires.

Scott nous dit que la méthode classique pour montrer qu'une formule ne dérive pas d'un système d'axiomes donné est d'exhiber un modèle où les axiomes sont *vrais* mais la formule *fausse*. C'est ce qu'il a fait; cependant, cela nécessite une réinterprétation de la logique pour ce qu'il souhaite faire. Il précise que ça n'est pas non plus trop artificiel, puisqu'il va considérer des événements dans un espace de probabilités.

Soit $(\Omega, \mathscr{A}, P)$ un espace de probabilité dans le sens commun, $\mathscr{A}$ étant une tribu, Ω un univers et P une mesure *positive* tel que $P(\Omega) = 1$. $\mathbb{R}$ sont les réels ordinaires, et appelons $\mathscr{R}$ les réels *aléatoires*. Les éléments de $\mathscr{R}$ sont les fonctions de $\Omega \rightarrow \mathbb{R}$ tel que $\forall r \in \mathbb{R}$:

$$\{\omega \in \Omega : \xi(\omega) \leq r\} \in \mathscr{A}$$

Les réels *ordinaires* peuvent être identifiés avec les fonctions constantes de cet espace. Le $0, 1, +$ ainsi que le produit sont interprétés de manière habituelle.

Cependant, dans les cas de l'égalité ou de l'ordre, il y a plus de choses à étudier. En effet, si nous marquons :

$$\mu = \xi$$

avec $\mu, \xi \in \mathscr{R}$, cette égalité n'est peut être pas toujours vraie.

Pour cela, Scott introduit l'algèbre de Boole suivante :

$$\mathscr{B} = \mathscr{A}/[P = 0]$$

qui n'est rien d'autre que la tribu quotienté par les évenements de $\mathscr{A}$ qui ont une mesure nulle pour P. Cela a pour effet d'éliminer la distinction entre "*presque-partout*" et "*partout*". De plus, Scott souligne que $\mathscr{B}$ est une algèbre de Boole complète. En effet, les propriétés de la tribu $\mathscr{A}$ sont conservées malgré le quotient. De plus, par le fait que la mesure soit positive (i.e. $P(\bigcup_{k\geq 1} E_k) = \sum_{k\geq 1} P(E_k)$ pour les unions dénombrables) implique que la condition de chaîne dénombrable est respectée (i.e. qu'il y a un nombre au plus dénombrable d'éléments disjoints deux à deux). C'est le cas, car si il existe une famille d'éléments disjoints deux à deux, dénombrable, nous aurions une mesure infinie (somme infinie de termes positifs); ce qui est donc impossible.

Sur cet ensemble, nous pouvons définir les symboles $\bigcup, \bigcap, \sim, \mathbb{0}, \mathbb{1}$ comme étant la réunion (autrement dit le *sup*), l'intersection (autrement dit l'*inf*), la négation comme le complément. Pour le $\mathbb{0}, \mathbb{1}$, ils sont définis tel que :

$$\mathbb{0} = \emptyset/[P = 0]$$
$$\mathbb{1} = \Omega/[P = 0]$$

De manière générale, la propriété suivante n'est pas vraie :

$$\bigcup_{i\in I}(E_i/[P = 0]) = (\bigcup_{i\in I})/[P = 0]$$

Elle l'est si I est dénombrable, par propriété directe des tribus. Cependant, il est à noter que la partie gauche est toujours dans $\mathscr{A}$, contrairement à droite (car une tribu n'est pas forcément stable par réunion indénombrable). Pour pallier à cela, Scott réinterprète $\mathscr{B}$ comme étant un système de *valeurs de vérités généralisé*. Le $\mathbb{0}$ et le $\mathbb{1}$ sont considérés comme respectivement le faux et le vrai, mais dans cette algèbre nous avons aussi des valeurs de vérités intermédiaires. Chaque déclaration, formule, aura une valeur de vérité dans cette algèbre; elle sera notée, pour disons une formule A : $[\![A]\!]$.

Par exemple, pour l'égalité $\xi = \eta$:

$$[\![\xi = \eta]\!] = \{\omega \in \Omega : \xi(\omega) = \eta(\omega)\} /[P = 0]$$

Pour $\xi \leq \eta$:

$$[\![\xi \leq \eta]\!] = \{\omega \in \Omega : \xi(\omega) \leq \eta(\omega)\} /[P = 0]$$

et enfin, l'addition $\xi + \eta = \sigma$:

$$[\![\xi + \eta = \sigma]\!] = \{\omega \in \Omega : \xi(\omega) + \eta(\omega) = \sigma(\omega)\} /[P = 0]$$

A partir de là, nous autorisons toutes les formes d'équations ou inégalités concernant des combinaisons polynômiales de réels *aléatoires*.

Soient A et B deux formules qui ont des valeurs de vérité bien définies dans l'algèbre de Boole. Nous introduisons alors des règles à propos de celles-ci :

$$\begin{aligned}
&[\![A \vee B]\!] = [\![A]\!] \bigcup [\![B]\!] \\
&[\![A \wedge B]\!] = [\![A]\!] \bigcap [\![B]\!] \\
&[\![\neg A]\!] = \sim [\![A]\!] \\
&[\![A \to B]\!] = [\![A]\!] \Rightarrow [\![B]\!] \\
&[\![A \leftrightarrow B]\!] = [\![A]\!] \Leftrightarrow [\![B]\!]
\end{aligned}$$

L'analogie avec la logique classique peut aussi être faite. Pour $E_1, E_2 \in \mathscr{B}$:

$$\begin{aligned}
&(E_1 \Rightarrow E_2) = \sim E_1 \bigcup E_2 \\
&(E_1 \Leftrightarrow E_2) = (E_1 \Rightarrow E_2) \bigcap (E_2 \Rightarrow E_1)
\end{aligned}$$

A titre d'exemple, Scott montre que $[\![\xi \leq \eta \ \vee \ \eta \leq \xi]\!] = \mathbb{1}$. En effet, nous avons :

$\{\omega \in \Omega : \xi(\omega) \leq \eta(w)\} /[P = 0] \bigcup \{\omega \in \Omega : \eta(\omega) \leq \xi(w)\} /[P = 0]$
$= (\{\omega \in \Omega : \xi(\omega) \leq \eta(w)\} \bigcup \{\omega \in \Omega : \eta(\omega) \leq \xi(w)\})/[P = 0]$
(la réunion étant dénombrable)

Et il semble clair que :

$$(\{\omega \in \Omega : \xi(\omega) \leq \eta(w)\} \bigcup \{\omega \in \Omega : \eta(\omega) \leq \xi(w)\}) = \Omega$$

Ce sont des bien des réels ordinaires qui sont comparés ici !

Chaque partie de cette disjonction doit donc être "*suffisament*" vraie pour que le tout est comme valeur de vérité $\mathbb{1}$.

Nous pouvons séparer les formules en deux catégories: celles avec des quantificateurs, et les autres.

S'il n'y en a pas, de manière similaire avec les réels *ordinaires*, l'associativité, la commutativité et la distributivité des lois $+, .$ et les lois concernant les éléments neutres, ainsi que la relation d'ordre (transitivité,..) sont conservés.

Pour les formules munies d'un quantificateur, nous regardons d'abord comment la formule serait quantifiée en fonction de variables réelles. De là, Scott a déduit que le quantificateur "*pour tout*" était probablement une *conjonction*, et que le "*il existe*" une disjonction. Nous pouvons alors noter :

$$[\![\forall x \ A(x)]\!] = \bigcap_{\xi \in \mathscr{R}} [\![A(\xi)]\!]$$
$$[\![\exists x \ A(x)]\!] = \bigcup_{\xi \in \mathscr{R}} [\![A(\xi)]\!]$$

Il est important de noter qu'une intersection (ou conjonction) ne vaudra $\mathbb{1}$ si et seulement si tous les éléments de la réunion valent $\mathbb{1}$. Pour la réunion, si l'un des termes est égal à $\mathbb{1}$, le *sup* vaudra $\mathbb{1}$. La première chose (légèrement) contre-intuitive est le fait qu'une disjonction peut valoir $\mathbb{1}$ (i.e. une vérité *absolue*) sans qu'aucun des termes ne soit *vraiment* vrais.

Regardons maintenant le comportement des réels aléatoires avec l'addition.

Typiquement, pour les réels, nous savons que :

$$\forall x \ \exists y \ [x + y = 0]$$

Comme dit précédemment, dans cette algèbre de Boole, il suffit *qu'une seule* valeur de vérité soit égale à $\mathbb{1}$ pour que le *sup* vale $\mathbb{1}$. Nous pouvons alors affirmer que, $\forall \xi \in \mathscr{R}, \ \exists \eta \in \mathscr{R}$:

$$[\![\xi + \eta = 0]\!] = \mathbb{1}$$

Scott généralise ce principe. Il prend une formule A, sans quantificateurs, de la forme :

$$\forall x_0 \ \forall x_1 \ \cdots \ \forall x_{n-1} \ \exists y \ A(x_0, x_1, \cdots, x_{n-1})$$

Alors, s'il existe une fonction mesurable φ tel que : $\forall (r_0, r_1, \cdots, r_{n-1}) \in \mathbb{R}^n$

Si la formule $A(x_0, x_1, \cdots, x_{n-1}, \varphi(x_0, x_1, \cdots, x_{n-1}))$ est vraie, alors :

$$[\![A(\xi_0, \xi_1, \cdots, \xi_{n-1}, \varphi(\xi_0, \xi_1, \cdots, \xi_{n-1}))]\!] = \mathbb{1}$$

En effet, il suffit de prendre $\eta = \varphi(\xi_0, \xi_1, \cdots, \xi_{n-1})$. Moyennant cette égalité, toutes les opérations qui sont faites de manière mesurables ont une valeur de vérité égale à $\mathbb{1}$ dans notre algèbre; en particulier pour les axiomes (OF), qui sont la pour vérifier si nos éléments peuvent bien être ordonnés. Nous pouvons noter que les quantificateurs $\exists$ et $\forall$ sur les réels aléatoires peuvent être vus comme des fonctions **mesurables**.

La notion de mesurable est très importante dans cette preuve. Sans ça, les notions d'égalités, d'inégalités, etc ne sont plus du tout valides, et des comportements indésirables apparaissent. De plus, la fin de la preuve est justement basée sur le fait que les fonctions considérées soient mesurables.

Scott formalise ensuite sa notion de vérité. Nous allons dire qu'une formule est *valide* si sa valeur dans l'algèbre de Boole est $\mathbb{1}$. Jusqu'à présent, la plupart des propriétés qui étaient vraies sur les réels *ordinaires* l'étaient pour les réels *aléatoires*. Cependant, et là vient remettre en question la définition de modèle dans ce cadre là, concernant la division, nous pourrions avoir que $\xi \cdot \eta = 0$ *p.p.* sans avoir pour autant $\xi = 0$ *ou* $\eta = 0$ *p.p.*. De ce fait, les réels *aléatoires* (pris avec le modulo des ensembles de mesure nulle) en tant qu'anneau ne représentent pas un modèle, en tout cas dans le sens "classique" du terme.

Néanmoins, Scott nous dit que si l'on associe une valeur booléenne à chaque formule, les réels *aléatoires* peuvent représenter un modèle pour les ensemble ordonnés. Pour cela, il en vient à discuter des axiomes de logique.

Il commence par dire que si l'un des axiomes vient de (PL), alors il est valide (c'est un théorème : ces règles de logique propositionnelle sont valides peu importe l'algèbre de Boole).

Ensuite, Scott fait la distinction entre ce qu'il appelle *sentence* (formule logique sans variables libres ou nouvelles notations) et *statement* (formule logique sans variables libres mais avec des noms, i.e. ce qu'il appelle des constantes). La théorie axiomatique s'intéresse seulement aux *sentences*. Cependant, afin de déterminer ce qui est valide dans notre modèle, nous avons besoin d'utiliser ces *sentences* à propros de ses éléments (au modèle). Dans la théorie axiomatique, quelques formules possèdent des variables libres, mais ça n'est pas un souci : nous pouvons toujours mettre des quantificateurs devant. De maniière similaire, une formule avec des variables libres est valide dans notre modèle si elle est valide peu importe la substitution des dites variables.

Là est dit quelque chose qui va être important pour la suite : pour montrer qu'une implication est valide, il suffit de montrer que sa valeur dans l'algèbre de Boole est inclue dans celle de sa conclusion (et donc, nous pouvons voir **l'implication comme une inclusion**).

Il prend pour exemple l'axiome typique pour le quantificateur $\forall$:

$$\forall x \ A(x) \to A((y + f(z)))$$

Même si la notion de fonction n'a pas été encore abordée dans ce modèle, disons que $\xi_0 = y + f(z)$ (c'est une varibale libre, c'est de la substitution).

Alors l'hypothèse s'écrit :

$$\bigcap_{\xi \in \mathscr{R}} [\![A(\xi)]\!]$$

et la conclusion :

$$[\![A(\xi_0)]\!]$$

Dès lors, on voit bien que l'hypothèse est inclue dans la conclusion (puisque c'est vrai *pour tout* $\xi \in \mathscr{R}$). Les autres règles de logique se prouvent de manière analogue.

2.3.2 Concept de fonctions aléatoires et fonctionnelles

Dans la partie précédente, nous avons vu que les fonctions des réels *ordinaires* peuvent naturellement s'étendre sur les fonctions des réels *aléatoires*.

Supposons:

$$\varphi : \mathbb{R} \to \mathbb{R}$$

une fonction mesurable; nous pouvons noter, de la même manière:

$$\varphi : \mathscr{R} \to \mathscr{R}$$

son extension aux réels *aléatoires*. Il est à noter que cette extension est une fonctionnelle, c'est à dire que $\varphi \circ \xi$ *pour* $\xi \in \mathscr{R}$ est une fonction de $\Omega \to \mathbb{R}$.

La propriété qui nous intéresse particulièrement pour ces fonctions est la notion d'égalité. Pour ξ, $\eta \in \mathscr{R}$, on a :

$$[\![\xi = \eta]\!] \subseteq [\![\varphi(\xi) = \varphi(\eta)]\!] \quad (\Delta)$$

Cette propriété découle directement des axiomes logiques d'égalité suivants:

$$\begin{array}{ll} (EL) & x = x \\ & x = y \to [A(x) = A(y)] \end{array}$$

A étant une formule logique arbitraire.

(EL) implique la formule (sur les réels):

$$[x = y \to f(x) = f(y)]$$

Par définition: $[\![\xi = \eta]\!] = \{\omega \in \Omega : \xi(\omega) = \eta(\omega)\} / [P = 0]$. Alors, en composant $\xi(\omega) = \eta(\omega)$ par φ, $\varphi \circ \xi(\omega) = \varphi \circ \eta(\omega)$.

Les fonctions φ ne peuvent donc pas rendre "moins" égales deux réels *aléatoires* qu'ils ne le sont déjà. Néanmoins, la nécessité d'être mesurable intervient à ce niveau: certaines fonctions *non*-mesurables peuvent ne pas satisfaire (Δ).

De manière analogue, les fonctions (toujours mesurables) $\psi : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ peuvent être étendues de la même façon. Posons $\psi : \mathscr{R} \times \mathscr{R} \to \mathscr{R}$ et prenons $\eta_0 \in \mathscr{R}$. Dès lors, φ peut être défini par:

$$\varphi(\xi) = \psi(\xi,\ \eta_0), \quad \forall \xi \in \mathscr{R}$$

Pour les mêmes raisons, ce φ ainsi défini respecte aussi la propriété (Δ).

La notion de fonctions *aléatoires* a aussi besoin d'être définie. En vertu des axiomes d'égalité, mais cette fois-ci pour les fonctions:

$$\begin{aligned} (EF) \quad f = g &\leftrightarrow \forall x[f(x) = g(x)] \\ F = G &\leftrightarrow \forall f[F(f) = G(f)] \end{aligned}$$

Nous pouvons définir:

$$[\![\varphi = \psi]\!] = \bigcap_{\xi \in \mathscr{R}} [\![\varphi(\xi) = \psi(\xi)]\!], \quad \forall \varphi, \psi \in \mathscr{R}^{\mathscr{R}}$$

Ce qui, entre d'autres termes : deux fonctions de $\mathscr{R} \to \mathscr{R}$ sont dites égales sur $A \subset \Omega$ si:

$$\varphi \circ \xi(\omega) = \psi \circ \xi(\omega) \quad p.p. \quad \forall \xi \in \mathscr{R},\, \forall \omega \in A$$

Ainsi, pour les fonctionnelles (i.e. les fonctions $\Phi : \mathscr{R}^{\mathscr{R}} \to \mathscr{R}$), une autre propriété très analogue à (Δ) est vérifiée :

$$[\![\varphi = \psi]\!] \subseteq [\![\Phi(\varphi) = \Phi(\psi)]\!] \quad (\Delta')$$

Naturellement, pour $\Phi, \Psi \in \mathscr{R}^{\mathscr{R}^{\mathscr{R}}}$ l'égalité entre deux fonctions *aléatoires* est définie de cette manière:

$$[\![\Phi = \Psi]\!] = \bigcap_{\varphi \in \mathscr{R}^{\mathscr{R}}} [\![\Phi(\varphi) = \Psi(\varphi)]\!]$$

Cela est applicable à tous les ordres: pour les fonctions $\Theta \in \mathscr{R}^{\mathscr{R}^{\mathscr{R}^{\mathscr{R}}}}$, etc..

Ces propriétés d'égalité nous affirment que les valeurs des fonctions ne dépendent que de leurs arguments; ce qui est suffisant pour cette preuve.

De manière générale, afin d'avoir un schéma axiomatique suffisant, nous pouvons considérer seulement les 12 suivants :

$$
\begin{aligned}
&1.x = y \rightarrow (x = z \leftrightarrow y = z)\\
&2.x = y \rightarrow (z = x \leftrightarrow z = y)\\
&3.x = y \rightarrow (x \leq z \leftrightarrow y \leq z)\\
&4.x = y \rightarrow (z \leq x \leftrightarrow z \leq y)\\
&5.x = y \rightarrow (x + z = y + z)\\
&6.x = y \rightarrow (z + x = z + y)\\
&7.x = y \rightarrow (x \cdot z = y \cdot z)\\
&8.x = y \rightarrow (z \cdot x = z \cdot y)\\
&9.x = y \rightarrow (f(x) = f(y))\\
&10.f = g \rightarrow (f(z) = g(z))\\
&11.f = g \rightarrow (F(f) = F(g))\\
&12.F = G \rightarrow (F(f) = G(f))
\end{aligned}
$$

Les 8 premiers sont valides en vertu du travail effectué précédemment. Quant aux 4 derniers, ils le sont par définition. Ainsi, tous les cas d'égalités peuvent être substituer par une combinaison (moyennant les règles de logique classique) de ces axiomes.

2.3.3 Preuve de la validité de l'axiome du choix (AC) dans le modèle

Étudions maintenant la validité de l'axiome du choix dans ce nouveau modèle, qui est moins évidente que les axiomes énoncés auparavant.

Rappelons l'axiome du choix:

$$
\begin{aligned}
(AC) \quad & \forall x\, \exists y\, A(x,y) \rightarrow \exists f\, \forall x\, A(x, f(x)) && (1)\\
& \forall f\, \exists y\, B(f,y) \rightarrow \exists F\, \forall f\, B(f, F(f)) && (2)
\end{aligned}
$$

Pour vérifier $(AC)(1)$, posons la $A'(x,y)$:

$$\forall x_0\, \exists y_0\, A(x_0, y_0) \rightarrow A(x,y)$$

Par les règles de la logique classique, la formule $\forall x \exists y A'(x,y)$ est valide (pour l'implication, les quantificateurs à droite peuvent être sortis de la formule).

Ainsi, la formule:

$$\exists f\, \forall x\, A'(x, f(x))$$

est parfaitement équivalent à (AC)(1). Ainsi, si quelque soit la formule B nous montrons que:

Si $\forall x\, \exists y\, B(x,y)$ est valide, alors $\exists f\, \forall x\, B(x, f(x))$ l'est aussi; elle le sera en particulier dans le cas où $B = A'$. (Σ)

Soit $\{\xi_\alpha : \alpha < \rho\}$ un bon ordre sur $\mathscr{R}$. L'axiome du choix est ici invoqué. L'existence de ce bon ordre est la conséquence du théorème de Zermelo, qui énonce que:

Théorème de Zermelo: Tout ensemble peut être muni d'une structure de bon ordre.

Pour montrer (Σ), supposons donc que $\forall x\, \exists y\, A(x,y)$ est valide, i.e. $\forall \alpha < \rho$:

$$[\![\exists \beta < \rho \;\; A(\xi_\alpha, \xi_\beta)]\!] = \mathbb{1}$$

Qui peut s'écrire :

$$\forall \alpha < \rho : \quad \bigcup_{\beta < \rho} [\![A(\xi_\alpha, \xi_\beta]\!] = \mathbb{1} \quad (\theta)$$

Soit $E_{\alpha\beta} \in \mathscr{B}$ tel que:

$$E_{\alpha\beta} = [\![A(\xi_\alpha, \xi_\beta)]\!] \sim \bigcup_{\gamma < \beta} [\![A(\xi_\alpha, \xi_\gamma)]\!]$$

Alors, pour un α fixé, la famille $\{E_{\alpha\beta} : \beta < \rho\}$ est une partition de $\mathbb{1}$ d'événements disjoints deux à deux.

En effet, pour $\beta' < \beta$, on a:

$$E_{\alpha\beta'} \subseteq \bigcup_{\gamma < \beta} [\![A(\xi_\alpha, \xi_\gamma)]\!]$$

d'où le fait que $E_{\alpha\beta'} \cap E_{\alpha\beta} = \emptyset$

De plus, la réunion recouvre bien tout l'ensemble $\mathbb{1}$ directement grâce à (θ).

Maintenant, pour justifier l'existence d'un telle fonction (pour montrer (Σ)), prouvons le lemme:

Lemme: $\forall \alpha < \rho$, $\exists\, \eta_\alpha \in \mathscr{R}$ *tel que* $:\ \forall \beta < \rho \quad E_{\alpha\beta} \subseteq [\![\eta_\alpha = \xi_\beta]\!]$

Preuve: Etant donné qu'il y a un ensemble au plus dénombrable d'évenements $E_{\alpha\beta}$ non égale à $\mathbb{0}$ (dû à (Σ)), à l'aide de l'axiome du choix, nous pouvons trouver une partition de Ω avec une famille :

$$\{\Lambda_{\alpha\beta} : \beta < \rho\} \quad avec \quad \forall \beta < \rho : \ E_{\alpha\beta} = \Lambda_{\alpha\beta}/[P = 0]$$

En d'autres termes, un $\Lambda_{\alpha\beta}$ est choisi dans la classe d'équivalence de $E_{\alpha\beta}$, tout en formant une partition de Ω.

Ensuite, définissons $\eta_\alpha : \Omega \to \mathbb{R}$ tel que $\forall \beta < \rho$:

$$\eta_{\alpha\,|\Lambda_{\alpha\beta}} = \xi_\beta|_{\Lambda_{\alpha\beta}}$$

L'application η_α prend bien des éléments de Ω du fait de la partition de cette famille, et pour un α fixé, elle nous permet de définir une fonction. Le lemme est ainsi prouvé.

Néanmoins, il reste du travail pour arriver à montrer que l'axiome du choix est valide dans notre modèle.

Soit $\varphi : \mathscr{R} \to \mathscr{R}$ tel que $\varphi(\xi_\alpha) = \eta_\alpha$. Si l'on veut montrer que $\varphi \in \mathscr{R}^{\mathscr{R}}$, nous devons montrer que :

$$[\![\xi_{\alpha_1} = \xi_{\alpha_2}]\!] \subseteq [\![\eta_{\alpha_1} = \eta_{\alpha_2}]\!] = [\![\varphi(\xi_{\alpha_1}) = \varphi(\xi_{\alpha_2})]\!] \quad \forall \alpha_1, \alpha_2 < \rho$$

En effet, cette contrainte supplémentaire sur les réels aléatoires (définie auparavant) est encore à vérifier.

A l'aide de l'axiome $(EL)(2)$ et par définition des $E_{\alpha\beta}$, pour un β fixé, on a bien :

$$[\![\xi_{\alpha_1} = \xi_{\alpha_2}]\!] \subseteq (E_{\alpha_1\beta} \Longleftrightarrow E_{\alpha_2\beta}) \quad (\Sigma')$$

Par le lemme, nous savons que $E_{\alpha_1\beta} \subseteq [\![\eta_{\alpha_1} = \xi_\beta]\!]$ et que $E_{\alpha_2\beta} \subseteq [\![\eta_{\alpha_2} = \xi_\beta]\!]$. Sachant (Σ'), nous pouvons affirmer que:

$$[\![\xi_{\alpha_1} = \xi_{\alpha_2}]\!] \cap E_{\alpha_1\beta} \subseteq [\![\eta_{\alpha_1} = \xi_\beta]\!] \cap [\![\eta_{\alpha_2} = \xi_\beta]\!]$$

De plus, il est clair que :

$$[\![\eta_{\alpha_1} = \xi_\beta]\!] \cap [\![\eta_{\alpha_2} = \xi_\beta]\!] \subseteq [\![\eta_{\alpha_1} = \eta_{\alpha_2}]\!]$$

Par conséquent :

$$[\xi_{\alpha_1} = \xi_{\alpha_2}]\!] \cap E_{\alpha_1\beta} \subseteq [\![\eta_{\alpha_1} = \eta_{\alpha_2}]\!]$$

Finalement, pour s'affranchir du β, en passant au *sup* dessus (i.e. le $E_{\alpha\beta}$ passe en $\mathbb{1}$ dû au fait que la famille forme une partition de $\mathbb{1}$), on obtient bien le résultat attendu.

De plus, le lemme nous dit aussi que :

$$E_{\alpha\beta} \subseteq [\![A(\xi_\alpha, \eta_\alpha)]\!] \quad (\Delta'')$$

car

$$E_{\alpha\beta} \subseteq [\![\eta_\alpha = \xi_\beta]\!] \quad (lemme)$$

et

$$E_{\alpha\beta} \subseteq [\![A(\xi_\alpha, \xi_\beta)]\!] \quad (definition)$$

et comme

$$[\![A(\xi_\alpha, \xi_\beta)]\!] \cap [\![\eta_\alpha = \xi_\beta]\!] \subseteq [\![A(\xi_\alpha, \eta_\alpha)]\!]$$

On a bien le résultat (Δ''). Dans (Δ''), si nous passons au *sup* sur β (comme précédemment, le $E_{\alpha\beta}$ passe en $\mathbb{1}$), nous avons :

$$\mathbb{1} \subseteq [\![A(\xi_\alpha, \varphi(\xi_\alpha))]\!]$$

Dès lors:

$$[\![A(\xi_\alpha, \varphi(\xi_\alpha))]\!] = \mathbb{1}$$

Cette formule est donc valide et cela $\forall \alpha < \rho$, qui définit notre ordre sur $\mathscr{R}$. Nous pouvons alors conclure que $\forall \xi \in \mathscr{R}$, $[\![A(\xi_\alpha, \varphi(\xi_\alpha))]\!]$ est valide, et que donc, en particulier $\exists f\ \forall x\ A(x, f(x))$ est aussi valide.

La preuve pour démontrer la validité de $(AC)(2)$ (axiome du choix mais sur les fonctionnelles cette fois-ci) est analogue.

Une partie qui vise à montrer que le modèle en question respecte bien (CO) a été rédigée par Scott, mais qui n'est pas traitée dans ce rapport.

2.4 La négation de l'hypothèse du continu dans un modèle approprié

Jusqu'à présent, il n'y a pas eu de restrictions particulières sur notre espace de probabilité. Maintenant, Scott a voulu construire un modèle où justement, il pourrait montrer que dans celui-ci, la valeur de vérité de (CH'') est 0. Ceci serait possible si l'on trouve un espace où il y aurait suffisament de réels *aléatoires* distincts, mais pas trop. Il énonce alors l'idée de regarder un produit (assez "gros") d'espaces car les projections sur ceux-ci (que nous pouvons appeler *coordonées*) sont presque sûrement des fonctions indépendantes. Il définit alors:

$$\Omega = [0, 1]^I$$

avec [0,1] l'interval unité usuel de $\mathbb{R}$ et I un "*index set*" (pas trouvé de traduction française: c'est un ensemble d'indices qui sert à numéroter un autre ensemble) de cardinal strictement plus grand que $\mathbb{R}$ (qui est toujours possible; par exemple, en prenant les parties de $\mathbb{R}$, nous avons déjà un ensmble de cardinal strictement plus grand que $\mathbb{R}$).

La mesure de Lebesgue est utilisée sur $[0, 1]$, et P sera la mesure produit sur la tribu de sous-ensembles de Baire de Ω. Etant donné que sur chaque segment $[0, 1]$ la mesure de Lebesgues μ est choisie, la mesure produit est définie ainsi :

$$P : (\mu_1, X_1) \times (\mu_2, X_2) \times \cdots \to \mathbb{R}^+$$

tel que :

$$(\mu_0 \times \mu_1\ \cdots)(X_0 \times X_1 \times \cdots) = \prod_{i \in P} \mu(X_i)$$

avec $\quad \forall i \in P \subset I : X_i \subseteq [0, 1]_i$.

De plus, définissons $\forall i \in I : \quad \xi_i : \Omega \to [0, 1]$ la *i-ème* coordonnée des éléments de notre espace Ω. Ces fonctions sont bien des réels *aléatoires* puisque qu'elles sont mesurables.

Soit $i, j \in I$. On a :

$$[\![\xi_i = \xi_j]\!] = \{\omega \in \Omega : \ \xi_i(\omega) = \xi_j(\omega)\} / [P = 0] =_{not} \{\omega \in \Omega : \ \omega_i = \omega_j\} / [P = 0]$$

Si $i \neq j$, alors la diagonale est de mesure nulle. En effet, si on se ramène au cas $[0, 1]^2$, l'endroit où $\xi_i = \xi_j$ est exactement sur la diagonale, qui ne possède pas de surface et qui a donc une mesure nulle. De manière plus formelle, nous pouvons majorer la mesure de cette diagonale par la mesure d'une suite de sous-ensembles de $[0, 1]$, qui correspond pour un $n > 1$ fixé :

$$E_n = [0, 1/2^n] \bigcup (\bigcup_{k=1}^{n-1} [1/2^{k-1}, 1/2^k]) \bigcup [1/2^n, 1]$$

et qui a pour mesure : $\mu(E_n) = 1/2^n$

Il advient alors que:

$$[\![\xi_i = \xi_j]\!] = \mathbb{0}$$

Scott énonce ensuite les raisons pour lesquelles l'hypothèse du continu va échouer dans ce modèle, et c'est exactement lié à cette diagonale : elle n'est pas dénombrable mais n'est pas non plus égale à tout l'ensemble. En étendant nos valeurs de vérités de $\{\mathbb{0}, \mathbb{1}\}$ à $\mathscr{B}$, nous permettons aux nombres réels de subir une extension vers ces réels *aléatoires*. Au travers d'une extension contrôlée, i.e. avec la construction d'une algèbre de Boole à partir d'un produit d'espace qui respecte tout de même la *countable chain condition*, Scott a réussi à trouver des sous-ensembles intermédiaires de la "*bonne taille*".

Le sous-ensemble intermédiaire en question va être les zéros d'une fonctions sur les réels *aléatoires*, à savoir $\chi : \mathscr{R} \to \mathscr{R}$. Afin de construire une telle fonction, prenons un sous-ensemble $J \subset I$, indénombrable mais pas de même cardinal que I. Il est possible de prendre un tel ensemble car si I est de cardinal égal à $\aleph_k$, où $k > 1$, il suffit de prendre un J avec un cardinal qui se trouve entre $\aleph_k$ et $\aleph_1$.

Nous voulons que la fonction χ est la propriété suivante:

$$\chi(\xi_j) = \mathbb{1}_{j \in J} \quad (fonction\ indicatrice\ de\ J)$$

Ce seront les zéros de cette fonction qui feront échouer l'hypothèse du continu dans ce modèle.

Quelque soit $\xi \in \mathscr{R}$, nous définissons :

$$\bigcup_{j \in J} [\![\xi = \xi_j]\!] = \Lambda_\xi / [P = 0]$$

qui représente l'ensemble où ξ rencontre les éléments indéxés par J. Alors:

$$\chi(\xi)(\omega) = 0 \ si\ \omega \in \Lambda_\xi ; \ 1 \ sinon$$

Un tel χ est bien une fonction aléatoire. En effet, nous avons bien $\chi \in \mathscr{R}^{\mathscr{R}}$; et si $\xi_i = \xi_j$: dans le cas où $i \neq j$, alors $[\![\xi_i = \xi_j]\!] = \mathbb{O}$ et on a bien $[\![\xi_i = \xi_j]\!] \subseteq [\![\chi(\xi_i) = \chi(\xi_j)]\!]$. Sinon, si $i = j$, alors $[\![\xi_i = \xi_j]\!] \subseteq [\chi(\xi_i) = \chi(\xi_j) = \mathbb{1}_{i \in J}]\!]$

Par ailleurs, χ possède la propriété suivante :

$$\forall \xi \in \mathscr{R} : \quad [\![\chi(\xi) = 0]\!] = \bigcup_{j \in J} [\![\xi = \xi_j]\!]$$

(nous pouvons montrer cela en utilisant le fait que si $\chi(\xi) = 0$, alors $\exists j \in J$ tel que $\xi = \xi_j$ sur un $\Lambda_\xi/[P = 0]$, d'où l'inclusion directe. L'inclusion réciproque est plus immédiate avec la définition de χ.

Nous alons montrer que dans notre formulation de (CH''), les deux parties du "*ou*" ont des valeurs de vérité valant $\mathbb{O}$. La preuve sera ainsi terminée.

Montrons d'abord que (c'est la partie concernant le fait d'être indénombrable, la partie sur le fait de l'être sera traitée après):

$$[\![\exists g \; \forall y \; \exists x [\chi(x) = 0 \; \wedge \; y = g(x)]]\!] = \mathbb{O}$$

Raisonnons par l'absurde et prenons un $\Psi : \mathscr{R} \to \mathscr{R}$ (c'est le g) tel que :

$$[\![\; \forall y \; \exists x [\chi(x) = 0 \; \wedge \; y = \Psi(x)]]\!] = E \neq \mathbb{O}$$

Ainsi, nous avons $\forall i \in I$:

$$E \subseteq [\![\exists x [\chi(x) = 0 \; \wedge \; \xi_i = \Psi(x)]]\!]$$

(comme c'est vrai $\forall y$, ça l'est pour un ξ_i en particulier)

Or :

$$[\![\exists x [\chi(x) = 0 \; \wedge \; \xi_i = \Psi(x)]]\!] = \bigcup_{\xi \in \mathscr{R}} [\![\chi(\xi) = 0 \; \wedge \; \xi_i = \Psi(\xi)]\!]$$

en fixant le $\exists x$ (rappel: l'existence est vue comme une réunion, et le "*quelque soit*" comme une intersection dans ce modèle). Par définition de χ, nous pouvons alors dire :

$$\bigcup_{\xi \in \mathscr{R}} [\![\chi(\xi) = 0 \; \wedge \; \xi_i = \Psi(\xi)]\!] = \bigcup_{\xi \in \mathscr{R}} \bigcup_{j \in J} [\![\xi = \xi_j \; \wedge \; \xi_i = \Psi(\xi)]\!]$$

Et donc bien sûr :

$$\bigcup_{\xi \in \mathscr{R}} \bigcup_{j \in J} [\![\xi = \xi_j \; \wedge \; \xi_i = \Psi(\xi)]\!] = \bigcup_{j \in J} [\![\xi_i = \Psi(\xi_j)]\!]$$

Par conséquent, $\forall i \in I$, il y a un $j_i \in J$ où $E \cap [\![\xi_i = \Psi(\xi_j)]\!] \neq \mathbb{O}$. En effet, $E \neq \mathbb{O}$ par hypothèse et $[\![\xi_i = \Psi(\xi_j)]\!] \neq \mathbb{O}$ parce que nous venons de montrer que $E \subseteq [\![\xi_i = \Psi(\xi_{j_i})]\!]$. Etant donné que J a été choisi avec un cardinal plus petit que I, avec I indénombrable, il existe forcément un ensemble indénombrable tel que $K = \{i \in I :\ j_i = k\}$. En effet, I étant plus grand que J, plusieurs éléments de I s'envoient sur le même point de J, noté j_i. Alors, nous pouvons trouver au moins un ensemble K de la sorte, sinon I et J seraient de même cardinal, ce qui contredirait nos hypothèses.

Regardons maintenant les événements :

$$D_i = E \cap [\![\xi_i = \Psi(\xi_k)]\!] \quad \forall i \in I$$

sont tous différents de zéro (pour les raisons énoncées ci-dessus), disjoints deux à deux (pour $i \neq i'$, nous avons $D_i \cap D_{i'} = [\![\xi_i = \Psi(\xi_k)]\!] \cap [\![\xi_{i'} = \Psi(\xi_k)]\!] \subseteq [\![\xi_i = \xi_{i'}]\!] = \mathbb{O}$) et indénombrable (car indéxé par K). Cela contredit alors la condition de chaîne dénombrable sur $\mathscr{B}$, qui stipule qu'il y a un nombre au plus dénombrable d'éléments par pairs disjoints de $\mathscr{B}$. Nous obtenons donc une contradiction. Il advient alors que :

$$E = \mathbb{O}$$

Concernant l'autre partie de (CH''), i.e. $[\![\exists f\ \forall y\ [\chi(y) = 0\ \rightarrow \exists x\ [N(x)\ \wedge y = f(x)]]\ ]\!] = \mathbb{O}$, le raisonnement est très similaire. Il faut juste vérifier que :

$$[\![N(\xi)]\!] = \bigcup_{n \in \mathbb{N}} [\![\xi = n]\!]$$

Nous aurons bien que $(CH'') = \mathbb{O}$ et par conséquent, l'indépendance de l'hypothèse du continu.