Forcing de bas niveau

Jean-Louis Krivine

19 mars 2012

Remarque.
Le titre ne se réfère pas au niveau mathématique du présent texte ou du lecteur, mais au rang des ensembles considérés, qui est $\leq \omega + 3$. Cette limitation permet un exposé autonome en quelques pages.

Le langage logique est celui de la logique *du second ordre*, avec des symboles de fonctions et des variables et constantes de prédicat sur les individus.
Les seuls symboles logiques sont $\to, \forall$.

Définitions. $\bot \equiv \forall X\, X$; $\neg A \equiv A \to \bot$; $A \wedge B \equiv \neg(A, B \to \bot)$; $A \vee B \equiv \neg A, \neg B \to \bot$;
$\exists x\, A \equiv \neg\forall x \neg A$; $\exists X\, A \equiv \neg\forall X \neg A$; $t = u \equiv \forall X(Xt \to Xu)$.
On écrira $A_1, A_2, \ldots, A_k \to A$ pour $A_1 \to (A_2 \to (\ldots (A_k \to A)\ldots))$.
On écrira $\exists x\{A_1, \ldots, A_k\}$ pour $\forall x(A_1, \ldots, A_k \to \bot) \to \bot$ et de même pour $\exists X$.

On a les symboles de fonction $0, s$ et $\mathbf{1}, \wedge$ et les constantes de prédicat $\perp\!\!\!\perp$ (unaire) et ε (binaire) ; $\neg\perp\!\!\!\perp(p)$ est notée $\mathsf{C}[p]$ et se lit : *p est une condition non triviale.*

On a les axiomes :
$\forall x(sx \neq 0)$; $\forall x\forall y(sx = sy \to x = y)$;
$\forall x(\mathbf{1} \wedge x = x)$; $\forall x(x \wedge x = x)$; $\forall x\forall y(x \wedge y = y \wedge x)$; $\forall x\forall y\forall z(x \wedge (y \wedge z) = (x \wedge y) \wedge z)$;
$\neg\perp\!\!\!\perp(\mathbf{1})$; $\forall p\forall q(\perp\!\!\!\perp(p) \to \perp\!\!\!\perp(p \wedge q))$.

On définit donc une relation d'ordre $\leq$ en posant $p \leq q \equiv (p \wedge q = p)$ et une relation de préordre $\sqsubseteq$ en posant $p \sqsubseteq q \equiv \forall r(\perp\!\!\!\perp(q \wedge r) \to \perp\!\!\!\perp(p \wedge r))$. On a $\forall p\forall q(p \leq q \to p \sqsubseteq q)$.
$\mathsf{C}[p \wedge q]$ se lit : *p est compatible avec q*.

On a la formule $\mathrm{int}(x) \equiv \forall X[\forall y(Xy \to Xsy), X0 \to Xx]$.
La formule $\forall x(\mathrm{int}(x) \to F)$ est notée $\forall x^{\mathrm{int}}\, F$.

On désigne par $\mathscr{M}$ un modèle de la logique du second ordre (schéma de compréhension). Ce sera le modèle de départ pour les preuves de consistance relative.
Suivant les besoins, on ajoutera des symboles de fonction ou de prédicat et des axiomes.
L'ensemble d'individus de $\mathscr{M}$ (appelé aussi ensemble des *conditions*) est désigné par P.

Pour chaque variable X de prédicat n-aire, on fixe une variable X^+ de prédicat $(n+1)$-aire.
Pour chaque formule F, on définit ci-dessous deux formules $p \in \|F\|$ et $p \Vdash F$, avec une variable libre p en plus ; $p \in \|F\|$ se lit : *p s'oppose à F* ; $p \Vdash F$ se lit : *p force F*.

$p \Vdash F$ est $\forall q(q \in \|F\| \to \perp\!\!\!\perp(p \wedge q))$.
$p \in \|X(\vec{t})\|$ est $\neg X^+(p, \vec{t})$ si X est une variable de prédicat et $\vec{t}$ une suite de termes.
$p \in \|\mathsf{R}(\vec{t})\|$ est $\neg\mathsf{R}(\vec{t})$ si R est une constante de prédicat.
$p \in \|A \to B\|$ est $\exists q\exists r\{q \Vdash A, r \in \|B\|, p = q \wedge r\}$.

$p \in \|\forall x\, A\|$ est $\exists x(p \in \|A\|)$.
$p \in \|\forall X\, A\|$ est $\exists X^+(p \in \|A\|)$.

On montre facilement :
$p \Vdash X(\vec{t}) \equiv \forall q(\mathsf{C}[p \wedge q] \to X^+(q, \vec{t}))$ si X est une variable de prédicat ;
$p \Vdash \mathsf{R}(\vec{t}) \equiv \mathsf{C}[p] \to \mathsf{R}(\vec{t})$ si R est une constante de prédicat ;
$p \in \|\bot\| \equiv \top$; $p \Vdash \bot \equiv \perp\!\!\!\perp(p)$; $p \Vdash F \Rightarrow p \wedge q \Vdash F$; $p \in \|F\| \Rightarrow p \Vdash \neg F$;
$p \Vdash A \to B \equiv \forall q(q \Vdash A \to p \wedge q \Vdash B)$; $p \Vdash \neg A \equiv \forall q(\mathsf{C}[p \wedge q] \to q \not\Vdash A)$;
$p \Vdash \forall x\, A \equiv \forall x(p \Vdash A)$; $p \Vdash \forall X\, A \equiv \forall X^+(p \Vdash A)$.
$p \in \|A \to B\| \equiv (p \Vdash A) \wedge \exists q\{p \leq q, q \in \|B\|\}$.
$p \in \|A_1, \ldots, A_n \to B\| \equiv (p \Vdash A_1) \wedge \ldots \wedge (p \Vdash A_n) \wedge \exists q\{p \leq q, q \in \|B\|\}$.
$p \in \|A_1, \ldots, A_n \to \bot\| \equiv (p \Vdash A_1) \wedge \ldots \wedge (p \Vdash A_n)$.
$p \Vdash (A_1, \ldots, A_n \to B) \equiv \forall q(q \Vdash A_1, \ldots, q \Vdash A_n \to p \wedge q \Vdash B)$.

Lemme 1. $p \Vdash F$, $q \sqsubseteq p \Rightarrow q \Vdash F$.

Soit $r \in \|F\|$; on a $\neg\mathsf{C}[p \wedge r]$ par hypothèse sur p, donc on a $\neg\mathsf{C}[q \wedge r]$ puisque $q \sqsubseteq p$.
C.Q.F.D.

Lemme 2.
i) $p \in \|a = b\| \Leftrightarrow \mathsf{C}[p] \to a \neq b$.
ii) $p \Vdash a = b \Leftrightarrow \mathsf{C}[p] \to a = b$.

i) $a = b$ s'écrit $\forall X(Xa \to Xb)$, donc $p \in \|a = b\|$ s'écrit $\exists X^+ \exists q\{p \leq q, p \Vdash Xa, q \in \|Xb\|\}$ soit
$(\star)$ $\quad \exists X^+ \exists q\{p \leq q, \forall r(\mathsf{C}[p \wedge r] \to X^+(r, a)), \neg X^+(q, b)\}$.
Preuve de $\Rightarrow$.
En faisant $r = q$ dans $(\star)$, on obtient $\mathsf{C}[p] \to X^+(q, a)$ et $\neg X^+(q, b)$.
On en déduit $\mathsf{C}[p] \to a \neq b$.
Preuve de $\Leftarrow$.
On suppose $\mathsf{C}[p] \to a \neq b$ et on montre $(\star)$ en prenant $q = p$ et en posant $X^+(u, x) \equiv (x \neq b)$.
Il reste alors à montrer $\forall r(\mathsf{C}[p \wedge r] \to a \neq b)$, ce qui est l'hypothèse.

ii) $p \Vdash a = b$ s'écrit $\forall q(q \in \|a = b\| \to \perp\!\!\!\perp(p \wedge q))$, c'est-à-dire, d'après (i) :
$\forall q\big((\mathsf{C}[q] \to a \neq b) \to \perp\!\!\!\perp(p \wedge q)\big)$ ou encore $\forall q(a \neq b \to \perp\!\!\!\perp(p \wedge q))$, qui équivaut à $\mathsf{C}[p] \to a = b$.
C.Q.F.D.

Lemme 3. $p \Vdash \mathit{int}(a) \Leftrightarrow \mathsf{C}[p] \to \mathit{int}(a)$.

Preuve de $\Leftarrow$.
Si on a $\neg\mathsf{C}[p]$, alors $p \Vdash \bot$, donc $p \Vdash \mathrm{int}(a)$.
On suppose donc $\mathrm{int}(a)$ et on doit montrer $p \Vdash \mathrm{int}(a)$, ce qui s'écrit :
$(\star)$ $\quad \forall X^+ \forall q(q \Vdash \forall y(Xy \to Xsy), q \Vdash X0 \to p \wedge q \Vdash Xa)$.
Il suffit donc de montrer $\forall a^{\mathrm{int}}(p \wedge q \Vdash Xa)$ avec les hypothèses :
$q \Vdash \forall y(Xy \to Xsy)$ et $q \Vdash X0$.
En raisonnant par récurrence sur a, on doit montrer :

- $p \wedge q \Vdash X0$. Ceci se déduit immédiatement de $q \Vdash X0$.
- $\forall b(p \wedge q \Vdash Xb \to p \wedge q \Vdash Xsb)$.

On a, par hypothèse, $q \Vdash (Xb \to Xsb)$, c'est-à-dire $\forall r(r \Vdash Xb \to q \wedge r \Vdash Xsb)$.
D'où le résultat, en prenant $r = p \wedge q$.

Preuve de $\Rightarrow$.
On fait l'hypothèse $p \Vdash \mathrm{int}(a)$, c'est-à-dire $(\star)$.
On doit montrer $\mathsf{C}[p] \to \mathrm{int}(a)$, c'est-à-dire $\forall Y\big(\forall y(Yy \to Ysy), Y0, \mathsf{C}[p] \to Ya\big)$.
Pour cela, on applique l'hypothèse $(\star)$ avec $X^+(r,x) \equiv Yx$.
On a $q \Vdash Xy \equiv \forall r(\mathsf{C}[q \wedge r] \to Yy)$, autrement dit $q \Vdash Xy \equiv (\mathsf{C}[q] \to Yy)$.
Donc $q \Vdash \forall y(Xy \to Xsy) \equiv \forall y \forall r\big((\mathsf{C}[r] \to Yy), \mathsf{C}[q \wedge r] \to Ysy\big)$
qui équivaut à $\mathsf{C}[q] \to \forall y(Yy \to Ysy)$.
L'hypothèse $(\star)$ donne donc :
$\forall Y \forall q\big((\mathsf{C}[q] \to \forall y(Yy \to Ysy)), (\mathsf{C}[q] \to Y0), \mathsf{C}[p \wedge q] \to Ya\big)$.
En faisant $q = \mathbf{1}$, on en déduit le résultat voulu.
C.Q.F.D.

Une formule est dite *du premier ordre*, si elle est obtenue par les règles suivantes :
- $\mathsf{R}(t_1, \ldots, t_k)$, $\bot$, $t = u$, $\mathrm{int}(t)$ sont du premier ordre ; R est une constante de prédicat, t_i, t, u sont des termes.
- Si F, G sont du premier ordre, $F \to G$ et $\forall x F$ le sont également.

Théorème 4. *Si F est une formule du premier ordre, alors $p \Vdash F$ équivaut à $\mathsf{C}[p] \to F$.*

Preuve par induction sur F. Le seul cas à examiner est $F \equiv A \to B$.
Alors, $p \Vdash A \to B$ est $\forall q(q \Vdash A \to p \wedge q \Vdash B)$ qui équivaut, par hypothèse d'induction à :
$\forall q\big((\mathsf{C}[q] \to A) \to (\mathsf{C}[p \wedge q] \to B)\big)$. Or, on a trivialement $\neg\mathsf{C}[q] \to (\mathsf{C}[p \wedge q] \to B)$.
Donc $p \Vdash (A \to B)$ équivaut à $\forall q\big(A \to (\mathsf{C}[p \wedge q] \to B)\big)$, c'est-à-dire $\mathsf{C}[p] \to (A \to B)$.
C.Q.F.D.

Lemme 5.
i) Si A est une formule du premier ordre, alors $p \Vdash (A \to B)$ équivaut à $A \to (p \Vdash B)$.
ii) $p \Vdash \forall n^{int} F[n]$ équivaut à $\forall n^{int}(p \Vdash F[n])$.

i) D'après le théorème 4, $p \Vdash (A \to B)$ équivaut à $\forall q((\mathsf{C}[q] \to A) \to p \wedge q \Vdash B)$.
Or, on a trivialement $\neg\mathsf{C}[q] \to (p \wedge q \Vdash B)$.
Donc $p \Vdash (A \to B)$ équivaut à $\forall q(A \to p \wedge q \Vdash B)$, c'est-à-dire $A \to (p \Vdash B)$.
ii) Corollaire de (i).
C.Q.F.D.

Lemme 6. $p \Vdash \exists \vec{x}\{F_1[\vec{x}], \ldots, F_k[\vec{x}]\}$ *équivaut à chacune des deux formules suivantes :*
$\forall q(\mathsf{C}[q], q \le p \to \exists \vec{x} \exists r\{\mathsf{C}[r], r \sqsubseteq q, (r \Vdash F_1[\vec{x}]), \ldots, (r \Vdash F_k[\vec{x}])\})$;
$\forall q(\mathsf{C}[q], q \sqsubseteq p \to \exists \vec{x} \exists r\{\mathsf{C}[r], r \le q, (r \Vdash F_1[\vec{x}]), \ldots, (r \Vdash F_k[\vec{x}])\})$.
Même énoncé en remplaçant $\exists \vec{x}$ par $\exists \vec{X}$.

Immédiat en écrivant la définition de $p \Vdash \forall \vec{x}(F_1[\vec{x}], \ldots, F_k[\vec{x}] \to \bot) \to \bot$.
C.Q.F.D.

Le modèle générique

Une partie $\mathscr{X}$ de P est dite :
- *saturée* si on a $\forall p \forall q(\mathscr{X}(p), q \le p \to \mathscr{X}(q))$; autrement dit $\forall p \forall q(\mathscr{X}(p) \to \mathscr{X}(p \wedge q))$;
- *prédense* si on a $\forall p(\mathsf{C}[p] \to \exists q\{\mathscr{X}(q), \mathsf{C}[p \wedge q]\})$;

• *dense* si $\forall p(\mathsf{C}[p] \to \exists q\{\mathscr{X}(q), \mathsf{C}[q], q \le p\})$; autrement dit :
$\forall p(\mathsf{C}[p] \to \exists q\{\mathscr{X}(p\wedge q), \mathsf{C}[p\wedge q]\})$.

Si $\mathscr{X}$ est prédense, alors $\exists q\{\mathscr{X}(q), p \le q\}$ définit une partie dense saturée.

Exemple. La formule $(p \Vdash F) \vee (p \Vdash \neg F)$ (lire : *p décide F*) définit une partie dense saturée de C.

On suppose maintenant le modèle $\mathscr{M}$ dénombrable (en prenant un sous-modèle élémentaire à l'aide du théorème de Löwenheim-Skolem).
Soit $\mathscr{X}_n \subset P$ une énumération des parties denses de P qui sont dans $\mathscr{M}$.
Une partie $\mathscr{G}$ de P est dite *générique* si :
$p, q \in \mathscr{G} \to \mathsf{C}[p\wedge q]$ (donc $\mathscr{G} \subset \mathsf{C}$) ; $p\wedge q \in \mathscr{G} \to p \in \mathscr{G}$; $\mathscr{G} \cap \mathscr{X}_n \neq \emptyset$ pour tout $n \in \mathbb{N}$.

Remarque. La fonction $n \mapsto \mathscr{X}_n$ et le générique $\mathscr{G}$ ne sont, en général, pas des prédicats du modèle $\mathscr{M}$.

Théorème 7 (Propriétés élémentaires du générique)**.**
i) Si $\mathscr{X}$ est prédense et dans $\mathscr{M}$, alors $\mathscr{G} \cap \mathscr{X} \neq \emptyset$. En particulier, on a $\mathbf{1} \in \mathscr{G}$.
ii) Si $p, q \in \mathscr{G}$, alors $p\wedge q \in \mathscr{G}$.
iii) Si tout élément de $\mathscr{G}$ est compatible avec p, alors $p \in \mathscr{G}$.
iv) $p \in \mathscr{G}, p \sqsubseteq q \;\Rightarrow\; q \in \mathscr{G}$.

i) $\exists q\{\mathscr{X}q, p \le q\}$ définit une partie dense saturée. Il existe donc p, q tels que :
$p \in \mathscr{G}, \mathscr{X}q, p \le q$; donc $q \in \mathscr{G}$.
ii) $\{r \in P ;\ \perp\!\!\!\perp(p\wedge r) \vee \perp\!\!\!\perp(q\wedge r) \vee r \le p\wedge q\}$ est dense.
iii) $\{q \in P ;\ \perp\!\!\!\perp(p\wedge q) \vee q \le p\}$ est dense.
iv) Corollaire de (iii).
C.Q.F.D.

Théorème 8. *Pour tout p tel que $\mathsf{C}[p]$, il existe un générique $\mathscr{G}$ tel que $p \in \mathscr{G}$.*

On définit une suite p_n, avec $p_0 = p$, $p_{n+1} \in \mathscr{X}_n, \mathsf{C}[p_{n+1}]$ et $p_{n+1} \le p_n$.
On pose $\mathscr{G} = \{q \in P ;\ (\exists n \in \mathbb{N})\ p_n \le q\}$.
C.Q.F.D.

Etant donné un générique $\mathscr{G}$, on définit un nouveau modèle $\mathscr{N}$ (noté aussi $\mathscr{M}[\mathscr{G}]$), dont l'ensemble d'individus est encore P. Un prédicat n-aire $\mathscr{X}$ de $\mathscr{N}$ est obtenu en prenant un prédicat $(n+1)$-aire $\mathscr{X}^+$ de $\mathscr{M}$ et en posant : $\quad \mathscr{X}(p_1, \ldots, p_n) \Leftrightarrow (\forall p \in \mathscr{G})\, \mathscr{X}^+(p, p_1, \ldots, p_n)$.
On considère chacun de ces prédicats $\mathscr{X}$ comme un nouveau symbole de relation et on étend la définition des formules $p \in \|F\|$ et $p \Vdash F$ à ce nouveau langage.
Lorsque F est une formule atomique de la forme $\mathscr{X}(\vec{t})$, on pose : $p \in \|\mathscr{X}(\vec{t})\| \equiv \neg\mathscr{X}^+(p, \vec{t})$
et on utilise ensuite la définition inductive de la page 1.
On a, en particulier : $p \Vdash \mathscr{X}(\vec{t}) \equiv \forall q\left(\mathsf{C}[p\wedge q] \to \mathscr{X}^+(q, \vec{t})\right)$.

Tous les prédicats de $\mathscr{M}$ sont dans $\mathscr{N}$ (on dit que $\mathscr{N}$ contient $\mathscr{M}$) : si $\mathscr{X}$ est un prédicat n-aire de $\mathscr{M}$, il suffit de poser $\mathscr{X}^+(p, p_1, \ldots, p_n) \equiv \mathscr{X}(p_1, \ldots, p_n)$.

Le générique $\mathscr{G}$ est, lui aussi, un prédicat du modèle $\mathscr{N}$. En effet, si on définit le prédicat binaire $\mathscr{G}^+(p, q) \equiv \mathsf{C}[p\wedge q]$, on a bien $\mathscr{G}(q) \Leftrightarrow (\forall p \in \mathscr{G})\mathsf{C}[p\wedge q]$ (théorème 7iii).

Remarque. On a $p \Vdash \mathscr{G}(q) \equiv \forall r(\mathsf{C}[p\wedge r] \to \mathscr{G}^+(r, q)) \equiv p \sqsubseteq q$.

Théorème 9 (Lemme de vérité)**.** *Pour toute formule close F à paramètres dans $\mathscr{N}$, on a :*
$\mathscr{N} \models F \;\Leftrightarrow\; (\exists p \in \mathscr{G})\mathscr{M} \models (p \Vdash F) \Leftrightarrow (\forall p \in \mathscr{G})\mathscr{M} \models (p \notin \|F\|)$.

On montre d'abord que $(\exists p \in \mathcal{G})\mathcal{M} \models (p \Vdash F) \Leftrightarrow (\forall p \in \mathcal{G})\mathcal{M} \models (p \notin \|F\|)$.
Preuve de $\Rightarrow$: Si $p \Vdash F$ et $q \in \|F\|$, alors on a $\neg \mathsf{C}[p \wedge q]$, donc on ne peut avoir $p, q \in \mathcal{G}$.
Preuve de $\Leftarrow$: $p \in \|F\| \vee p \Vdash F$ définit une partie prédense, par définition de $p \Vdash F$.

On prouve alors le théorème par récurrence sur F. Si F est atomique, il y a deux cas :
$F \equiv \mathcal{X}(\vec{t})$ où $\mathcal{X}$ est un prédicat de $\mathcal{N}$; on a alors :
$(\forall p \in \mathcal{G})(p \notin \|F\|) \Leftrightarrow (\forall p \in \mathcal{G})\mathcal{X}^+(p, \vec{t}) \Leftrightarrow \mathcal{N} \models \mathcal{X}(\vec{t})$.
$F \equiv \mathsf{R}(\vec{t})$ où R est un symbole de prédicat. Démonstration analogue.

Si $F \equiv A \to B$: on a $\mathcal{N} \not\models A \to B \Leftrightarrow (\mathcal{N} \models A) \wedge (\mathcal{N} \not\models B)$
$\Leftrightarrow (\exists p \in \mathcal{G})(\mathcal{M} \models p \Vdash A) \wedge (\exists q \in \mathcal{G})(\mathcal{M} \models q \in \|B\|)$ (par hypothèse de récurrence)
$\Leftrightarrow \exists p \exists q[(p \wedge q \in \mathcal{G}) \wedge (\mathcal{M} \models p \Vdash A) \wedge (\mathcal{M} \models q \in \|B\|)] \Leftrightarrow (\exists r \in \mathcal{G})(\mathcal{M} \models r \in \|A \to B\|)$.

Si $F \equiv \forall x\, A$: on a $\mathcal{N} \models \forall x\, A \Leftrightarrow \forall a(\mathcal{N} \models A[a/x]) \Leftrightarrow \forall a(\forall p \in \mathcal{G})(\mathcal{M} \models p \notin \|A[a/x]\|)$ (par hypothèse de récurrence) $\Leftrightarrow (\forall p \in \mathcal{G})(\mathcal{M} \models p \notin \|\forall x\, A\|)$.

Si $F \equiv \forall X\, A$, où X est n-aire : on a $\mathcal{N} \models \forall X\, A \Leftrightarrow$ pour tout $\mathcal{X}^+ \in \mathcal{P}(P^{n+1})$ $(\mathcal{N} \models A[\mathcal{X}]) \Leftrightarrow$ pour tout $\mathcal{X}^+ \in \mathcal{P}(P^{n+1})$ $(\forall p \in \mathcal{G})(\mathcal{M} \models p \notin \|A[\mathcal{X}]\|)$ (par hypothèse de récurrence)
$\Leftrightarrow (\forall p \in \mathcal{G})(\mathcal{M} \models p \notin \|\forall X\, A\|)$.

C.Q.F.D.

Théorème 10.
i) $\mathcal{N}$ est un modèle de la logique du second ordre (schéma de compréhension).
ii) Pour toute formule close F du premier ordre, à paramètres dans $\mathcal{M}$, on a $\mathcal{M} \models F \Leftrightarrow \mathcal{N} \models F$.

i) Soit $\forall \vec{x}\, F[\vec{x}]$ une formule close avec paramètres ; on définit le prédicat :
$\mathcal{X}^+(p, \vec{x}) \equiv p \notin \|F(\vec{x})\|$. On a alors :
$p \Vdash F(\vec{x}) \equiv \forall q(q \in \|F(\vec{x})\| \to \bot\!\!\!\bot(p \wedge q)) \equiv \forall q(\mathsf{C}[p \wedge q] \to \mathcal{X}^+(q, \vec{x})) \equiv p \Vdash \mathcal{X}(\vec{x})$.
Il en résulte que $\mathbf{1} \Vdash \forall \vec{x}(F(\vec{x}) \to \mathcal{X}(\vec{x}))$ et $\mathbf{1} \Vdash \forall \vec{x}(\mathcal{X}(\vec{x}) \to F(\vec{x}))$.
D'après le théorème 9, on a donc $\mathcal{N} \models \forall \vec{x}(F(\vec{x}) \to \mathcal{X}(\vec{x}))$ et $\mathcal{N} \models \forall \vec{x}(\mathcal{X}(\vec{x}) \to F(\vec{x}))$.

ii) Immédiat, d'après les théorèmes 4 et 9.

C.Q.F.D.

En particulier, $\mathcal{M}$ et $\mathcal{N}$ ont les mêmes entiers.

Bon ordre sur les individus

Théorème 11. *Soit $\lhd$ une relation binaire sur P, qui est bien fondée dans $\mathcal{M}$; alors $\lhd$ est bien fondée dans $\mathcal{N}$.*

On montre que $\mathbf{1} \Vdash \forall X\{\forall x[\forall y(y \lhd x \to Xy) \to Xx] \to \forall x\, Xx\}$. On fixe donc $x_0 \in P$ et un prédicat unaire $\mathcal{X}$ de $\mathcal{N}$, représenté par un prédicat binaire $\mathcal{X}^+$ de $\mathcal{M}$.
On suppose $p \Vdash \forall x[\forall y(y \lhd x \to \mathcal{X}y) \to \mathcal{X}x]$ et on montre $p \Vdash \mathcal{X}x_0$ par induction sur la relation bien fondée $\lhd$. D'après l'hypothèse sur p, il suffit de montrer $p \Vdash \forall y(y \lhd x_0 \to \mathcal{X}y)$, c'est-à-dire $\forall q \forall y(q \Vdash y \lhd x_0 \to p \wedge q \Vdash \mathcal{X}y)$.
Mais $y \lhd x_0$ est une formule atomique, donc du premier ordre ; par suite $q \Vdash y \lhd x_0$ est : $\mathsf{C}[q] \to y \lhd x_0$. Par hypothèse d'induction, on a $y \lhd x_0 \to p \Vdash \mathcal{X}y$, d'où le résultat.

C.Q.F.D.

Il en résulte que si $\mathcal{M}$ satisfait l'axiome : *Il existe un bon ordre sur les individus,* il en est de même pour $\mathcal{N}$.

L'axiome du choix dépendant (ACD)

On suppose maintenant que $P = \mathscr{P}(\mathbb{E})$ avec $\mathbb{E} \supset \mathbb{N}$; on définit une constante de prédicat binaire ε en posant : $p \varepsilon q \Leftrightarrow p \in \mathbb{N} \wedge p \in q$.
On ajoute les symboles de constante $\emptyset$ et $\mathbb{N}$, interprétés dans $P = \mathscr{P}(\mathbb{E})$ de façon évidente.
L'axiome suivant, appelé *représentation des parties de* $\mathbb{N}$ *(RPN)*, est satisfait dans $\mathscr{M}$:
$\forall X \exists x \forall n^{\text{int}}(Xn \leftrightarrow n \varepsilon x)$.
On choisit une bijection $\beta : \mathbb{N} \times \mathbb{E} \to \mathbb{E}$, dont la restriction à $\mathbb{N}^2$ est une bijection de $\mathbb{N}^2$ sur $\mathbb{N}$.
On définit $g : P^2 \to P$ en posant :
$g(n,p) = \{x \in \mathbb{E};\ \beta(n,x) \in p\}$ si $n \in \mathbb{N}$; $g(n,p) = \emptyset$ si $n \notin \mathbb{N}$.
On ajoute le symbole de fonction binaire g au langage, en écrivant p_n pour $g(n,p)$.
Toute suite d'individus (éléments de P) est ainsi représentée, d'une façon et d'une seule, par un individu. On a donc un *axiome d'extensionnalité (Ext)* :
$\forall p \forall q(\forall n^{\text{int}}(p_n = q_n) \to p = q)$.
L'axiome du choix dépendant (ACD) est la formule suivante :
$\forall X(\forall x \exists y\, X(x,y) \to \forall a \exists u\{u_0 = a, \forall n^{\text{int}}\, X(u_n, u_{n+1})\})$.
L'axiome du choix dénombrable (ACd) est la formule suivante :
$\forall X(\forall n^{\text{int}} \exists y\, X(n,y) \to \exists u \forall n^{\text{int}}\, X(n,u_n))$.
Ces deux axiomes sont satisfaits dans le modèle de base $\mathscr{M}$.
On définit le symbole de fonction binaire (p,q) pour le couple d'individu, dans le modèle de base $\mathscr{M}$ comme le seul individu r tel que $r_0 = p$ et $r_{n+1} = q$ pour tout $n \in \mathbb{N}$.
Les *axiomes du couple (Cpl)* suivants sont vérifiés :
$\forall p \forall q \forall p' \forall q'((p,q) = (p',q') \to p = p' \wedge q = q')$; $\forall p \forall q((p,q)_0 = p \wedge (p,q)_1 = q)$.
On ajoute le symbole de fonction unaire ζ, défini dans $\mathscr{M}$ par $\zeta(u) = \{n \in \mathbb{N};\ u_n = 0\}$.
L'axiome suivant est donc vérifié :
(Zéro) $\forall u \forall n^{\text{int}}(n \varepsilon \zeta(u) \leftrightarrow u_n = 0)$.

Théorème 12. *i) Cpl, ACD* $\vdash$ *ACd ; ii) Zéro, ACd* $\vdash$ *RPN.*

i) On suppose $\forall n^{\text{int}} \exists y\, \mathscr{X}(n,y)$; soit a tel que $\mathscr{X}(0,a)$. On applique ACD à la formule :
$\forall m \forall x \exists n \exists y\{(n = sm), (\text{int}(n) \to \mathscr{X}(n,y))\}$. On obtient donc une suite (m_i, u_i) telle que :
$(m_0, u_0) = (0,a)$, $m_{i+1} = sm_i$ et $\mathscr{X}(m_{i+1}, u_{i+1})$ pour tout $i \in \mathbb{N}$.
On a donc $m_i = i$, d'où $\mathscr{X}(i,u_i)$ pour tout $i \in \mathbb{N}$.

ii) Soit $\mathscr{X}$ un prédicat unaire ; on applique ACd à la formule :
$\forall n^{\text{int}} \exists y\{(\mathscr{X}n \to y = 0), (\neg \mathscr{X}n \to y = 1)\}$. On obtient donc $u \in P$ tel que $\forall n^{\text{int}}(\mathscr{X}n \leftrightarrow u_n = 0)$, d'où $\forall n^{\text{int}}(\mathscr{X}n \leftrightarrow n \varepsilon \zeta(u))$.

C.Q.F.D.

La condition de chaîne dénombrable décroissante (CCD)

CCD est la formule : $\forall u(\forall n^{\text{int}} \subset [u_n], \forall n^{\text{int}}(u_{n+1} \leq u_n) \to \exists p\{\subset [p], \forall n^{\text{int}}(p \sqsubseteq u_n)\})$;
c'est-à-dire :
Toute suite décroissante pour $\leq$ *d'éléments de* $\subset$ *a un minorant dans* $\subset$ *pour* $\sqsubseteq$.

Théorème 13. *Si* $\mathscr{M} \models$ *ACD et si la CCD est vérifiée dans* $\mathscr{M}$*, alors* $\mathscr{N} \models$ *ACD.*
Autrement dit : ACD, CCD $\vdash$ (**1** $\Vdash$ ACD).

On montre $\mathbf{1} \Vdash$ ACD dans $\mathscr{M}$. Soient donc $a, p \in P$ et $\mathscr{X}^+$ un prédicat ternaire de $\mathscr{M}$.
On suppose $p \Vdash \forall x \exists y \mathscr{X}(x,y)$ et on montre $p \Vdash \exists u\{u_0 = a, \forall n^{\text{int}} \mathscr{X}(u_n, u_{n+1})\}$, en appliquant le lemme 6. Soit donc $p' \leq p$ tel que $\mathsf{C}[p']$. On a $\forall x(p' \Vdash \exists y \mathscr{X}(x,y))$, c'est-à-dire, d'après le lemme 6 : $\forall x \forall q(\mathsf{C}[q], q \leq p' \to \exists y \exists r\{\mathsf{C}[r], r \leq q, r \Vdash \mathscr{X}(x,y)\})$.
En appliquant ACD, on obtient un couple (u,q) tel que $(u_0, q_0) = (a, p')$ et :
$\forall n^{\text{int}}(\mathsf{C}[q_n], q_n \leq p' \to \mathsf{C}[q_{n+1}] \wedge (q_{n+1} \leq q_n) \wedge q_{n+1} \Vdash \mathscr{X}(u_n, u_{n+1}))$.
En appliquant la CCD à la suite q_n, on obtient une condition $q \sqsubseteq q_n \leq p'$, telle que $\mathsf{C}[q]$.
On a donc $\forall n^{\text{int}}(q \Vdash \mathscr{X}(u_n, u_{n+1}))$ et donc $q \Vdash \forall n^{\text{int}} \mathscr{X}(u_n, u_{n+1})$, d'après le lemme 5(ii).
C.Q.F.D.

Théorème 14 (Conservation des réels)**.**
Si $\mathscr{M} \models$ ACD et si la CCD est vérifiée dans $\mathscr{M}$, alors $\mathscr{N} \models RPN$.
Tout ensemble d'entiers qui est dans $\mathscr{N}$ est donc déjà dans $\mathscr{M}$.

Corollaire des théorèmes 12 et 13.
C.Q.F.D.

Un ultrafiltre sur $\mathbb{N}$

Dans cet exemple et le suivant, le modèle de base $\mathscr{M}$ a $\mathscr{P}(\mathbb{N})$ comme ensemble d'individus. On pose donc $\mathbb{E} = \mathbb{N}$.
Pour $p, q \in P = \mathscr{P}(\mathbb{N})$, on pose $p \wedge q = p \cap q$ et $\mathbf{1} = \mathbb{N}$; $\mathsf{C}[p]$ est la formule $\forall i^{\text{int}} \exists j^{\text{int}}(i + j \,\varepsilon\, p)$ c'est-à-dire : *p est une partie infinie de* $\mathbb{N}$. Donc $p \leq q \equiv p \subset q$ et $p \sqsubseteq q \equiv (p \setminus q$ *est fini*$)$.

Lemme 15. *La condition de chaîne dénombrable décroissante est vérifiée.*

Soit p_n une suite décroissante pour $\subset$ telle que $\mathsf{C}[p_n]$. On définit $f : \mathbb{N} \to \mathbb{N}$ en posant :
$f(i) =$ le premier $j \,\varepsilon\, p_i, j > i$; on désigne par p l'image de f. Alors p est évidemment infini, d'où $\mathsf{C}[p]$. De plus, $p \setminus p_i$ est fini, car $\subset \{f(0), \ldots, f(i-1)\}$. On a donc $p \sqsubseteq p_i$ pour tout $i \in \mathbb{N}$.
C.Q.F.D.

Un générique $\mathscr{G}$ est, dans $\mathscr{N}$, un ultrafiltre non trivial sur l'ensemble des parties de $\mathbb{N}$ qui sont représentées par des individus. Mais, d'après le lemme 15 et le théorème 14, toute partie de $\mathbb{N}$ est, dans le modèle $\mathscr{N}$, représentée par un individu. Donc $\mathscr{N}$ satisfait la formule :
Il existe un ultrafiltre non trivial sur $\mathbb{N}$. On a montré le

Théorème 16. *Soit F une formule de l'arithmétique du second ordre, démontrable en arithmétique du 3ème ordre avec les axiomes : ACD et l'existence d'un ultrafiltre sur $\mathbb{N}$. Alors F est démontrable avec l'arithmétique du 3ème ordre et ACD.*

Exercice. Montrer que le générique $\mathscr{G}$ est, dans $\mathscr{N}$, un ultrafiltre *sélectif*, c'est-à-dire :
pour toute fonction $f : \mathbb{N} \to \mathbb{N}$, il existe un élément de l'ultrafiltre sur lequel f est, soit constante, soit strictement croissante.
Indication. Noter d'abord que la fonction f est dans $\mathscr{M}$; et ensuite que les parties infinies de $\mathbb{N}$, sur lesquelles f est, soit bornée, soit strictement croissante, forment une partie dense de C.
Remarque. L'existence d'un ultrafiltre sélectif est conséquence de l'hypothèse du continu, mais pas de l'axiome du choix.

L'hypothèse du continu

Soit $\mathscr{U}$ l'ensemble des couples (u,v) où u est une partie dénombrable ou finie de $\mathscr{P}(\mathbb{N})$ et v un bon ordre sur u. On se fixe une bijection $\varphi : \mathscr{P}(\mathbb{N}) \to \mathscr{U}_+$, où $\mathscr{U}_+$ est obtenu en ajoutant un élément $\mathbf{0}$ à $\mathscr{U}$. Cela va permettre de définir la structure de forcing $(\mathsf{C}, \wedge, \mathbf{1})$ sur $\mathscr{U}_+$ d'abord, puis de la transporter sur $P = \mathscr{P}(\mathbb{N})$ par la bijection φ. On utilisera les mêmes symboles $\mathsf{C}, \wedge, \mathbf{1}, \ldots$ sur $\mathscr{U}$ et sur P, ce qui ne devrait pas entrainer de confusion.

$\mathscr{U}$ est un arbre pour la relation d'ordre :
$(u,v) \leq (u',v') \Leftrightarrow (u',v')$ est un segment initial de (u,v) (on a donc $(u,v) \leq (u',v') \Rightarrow u' \subset u$).
On pose $\mathbf{1} = (\emptyset, \emptyset)$; $\perp\!\!\!\perp = \{\mathbf{0}\}$; pour $(u,v), (u',v') \in \mathscr{U}$, on pose $(u,v) \wedge (u',v') = \mathbf{0}$ sauf si :
ou bien $(u,v) \leq (u',v')$, et alors $(u,v) \wedge (u',v') = (u,v)$,
ou bien $(u',v') \leq (u,v)$, et alors $(u,v) \wedge (u',v') = (u',v')$.
On vérifie facilement la condition de chaîne dénombrable décroissante.
Soit $\mathscr{G} \subset P$ un générique ; alors la réunion G des éléments de $\varphi(\mathscr{G})$ est une partie de $\mathscr{P}(\mathbb{N})$ munie d'un bon ordre dont tous les segments initiaux sont dénombrables.
Soit $a \in \mathscr{P}(\mathbb{N})$; alors $\{(u,v) \in \mathscr{U} ;\ a \in u\}$ est dense : en effet, si on a $\mathsf{C}(u,v)$ et si $a \notin u$, on pose $u' = u \cup \{a\}$ et on prolonge le bon ordre v en v' de façon que a soit le plus grand élément de u' ; on a alors $(u',v') \leq (u,v)$.
Il en résulte que toute partie de $\mathbb{N}$, qui est représentée par un individu, est élément de G. D'après le lemme 15 et le théorème 14, G est donc, dans $\mathscr{N}$, l'ensemble de *toutes* les parties de $\mathbb{N}$. Dans le modèle $\mathscr{N}$, il existe donc un bon ordre sur $\mathscr{P}(\mathbb{N})$, dont tout segment initial est dénombrable. On a montré :

Théorème 17. *S'il existe un modèle de l'arithmétique du 3ème ordre qui satisfait ACD, alors il en existe un qui satisfait « il existe, sur $\mathscr{P}(\mathbb{N})$, un bon ordre dont tout segment initial est dénombrable » (hypothèse du continu).*

Théorème 18. *Soit F une formule de l'arithmétique du second ordre, démontrable en arithmétique du 3ème ordre avec l'hypothèse du continu. Alors F est démontrable avec l'arithmétique du 3ème ordre et ACD.*

On raisonne par l'absurde, en considérant un modèle $\mathscr{M}$ de l'arithmétique du 3ème ordre, qui satisfait ACD + $\neg F$. La formule F est une formule *du premier ordre*, suivant notre définition. Par suite, le modèle $\mathscr{N}$ satisfait aussi $\neg F$; cela contredit l'hypothèse, puisqu'il satisfait également l'arithmétique du 3ème ordre et l'hypothèse du continu.

C.Q.F.D.

La condition d'antichaîne dénombrable (CAD)

Ordinaux dénombrables

On définit les formules suivantes, où X, X' sont des variables de prédicat binaire :

• $\mathrm{BN}(X)$ (lire *"X est un bon ordre sur $\mathbb{N}$"*) est le triplet de formules :
$\forall U[\forall x(\forall y(X(y,x) \to Uy) \to Ux) \to \forall x\, Ux]$;
$\forall m \forall n(X(m,n) \to \mathrm{int}(m) \wedge \mathrm{int}(n))$; $\forall m^{\mathrm{int}} \forall n^{\mathrm{int}}(X(m,n) \vee X(n,m) \vee m = n)$;

Elles expriment que X est une relation binaire bien fondée, contenue dans $\mathbb{N}^2$ et totale.
Lorsque $X(m,n)$ est de la forme $(m,n)\,\varepsilon\,u$, on écrira $\mathrm{BN}(u)$ au lieu de $\mathrm{BN}(X)$.

• $X \simeq X'$ (lire *X est isomorphe à X'*) est la formule :
$\exists F\{\mathrm{Perm}(F), \forall m \forall n \forall m' \forall n' (F(m,m'), F(n,n') \to (X(m,n) \leftrightarrow X'(m',n')))\}$
où $\mathrm{Perm}(F)$ (lire *"F est une permutation de $\mathbb{N}$"*) est formé des trois formules :
$\forall m \forall n (F(m,n) \to \mathrm{int}(m) \wedge \mathrm{int}(n))$; $\forall m^{\mathrm{int}} \exists! n\, F(m,n)$; $\forall n^{\mathrm{int}} \exists! m\, F(m,n)$.
Lorsque $X(m,n)$ est de la forme $(m,n)\,\varepsilon\,u$, on écrira $u \simeq X'$ au lieu de $X \simeq X'$.
Si, de plus, $X'(m',n')$ est de la forme $(m',n')\,\varepsilon\,u'$, on écrira $u \simeq u'$ au lieu de $X \simeq X'$.

L'axiome OD des *ordinaux dénombrables* est la formule :
$\exists U(\forall v(\mathrm{BN}(v) \to \exists! u\{U u, u \simeq v\})$.
Le prédicat unaire U choisit donc un représentant de chacun des bons ordres sur $\mathbb{N}$ qui sont représentés par des individus.
Quand cet axiome est satisfait, on fixe un tel prédicat unaire noté Od, dont les éléments sont appelés *ordinaux dénombrables*.

Dans la suite, on suppose que le modèle de base $\mathscr{M}$ satisfait l'axiome du choix et donc, en particulier, cet axiome OD.
Tout modèle générique $\mathscr{N}$ satisfait alors aussi OD.
En effet, $\mathscr{N}$ contient $\mathscr{M}$ et a les mêmes individus que $\mathscr{M}$. De plus, toute relation binaire sur les individus qui est un bon ordre dans $\mathscr{M}$ est aussi un bon ordre dans $\mathscr{N}$ (théorème 11).

L'axiome suivant, noté RBN, est appelé *représentation des bons ordres sur $\mathbb{N}$* :
$\forall X(\mathrm{BN}(X) \to \exists u(X \simeq u))$.
Cet axiome exprime que *tout bon ordre sur $\mathbb{N}$ est représenté par un individu.*
Il est évidemment conséquence de RPN.
Les axiomes OD + RBN signifient donc :
Tout bon ordre sur $\mathbb{N}$ est isomorphe à un ordinal dénombrable et un seul.

La condition d'antichaîne dénombrable est la formule, notée CAD :
$\forall X(\mathrm{Atch}(X) \to \exists u \forall v(X v \to \exists n^{\mathrm{int}}(v = u_n))$
où $\mathrm{Atch}(X)$ (lire *"X est une antichaîne"*) est formé des deux formules :
$\forall u(X u \to \complement[u])$; $\forall u \forall v(X u, X v \to \perp\!\!\!\perp(u \wedge v))$.

Théorème 19 (Conservation des bons ordres sur $\mathbb{N}$)**.**
Si la CAD est vérifiée dans $\mathscr{M}$, alors $\mathscr{N} \models RBN$.
Tout bon ordre sur $\mathbb{N}$ qui est dans $\mathscr{N}$ est donc isomorphe (dans $\mathscr{N}$) à un bon ordre sur $\mathbb{N}$ qui est dans $\mathscr{M}$.

Soit B un prédicat binaire qui est un bon ordre sur $\mathbb{N}$ dans $\mathscr{N}$ et n'est pas représenté par un individu. On peut supposer que ce bon ordre est minimum, c'est-à-dire que tout segment initial propre $B_n = \{m \in \mathbb{N};\ B(m,n)\}$ est représenté par un individu, donc par un ordinal u_n puisque $\mathscr{N} \models \mathrm{OD}$. La fonction $n \mapsto u_n$ est un prédicat binaire F de $\mathscr{N}$.
Il existe donc une condition $p_0 \in \mathscr{G}$ telle que $p_0 \Vdash$ "F est une application de $\mathbb{N}$ dans Od".
Pour chaque $n \in \mathbb{N}$, soit $E_n = \{u; Od(u), (\exists p \leq p_0)\{\complement[p], p \Vdash F(n,u)\}\}$. L'application $n \mapsto E_n$ est définie dans $\mathscr{M}$ et E_n est dénombrable pour chaque $n \in E_n$:
en effet, si $p, p' \leq p_0, u \neq u', p \Vdash F(n,u), p' \Vdash F(n,u')$, alors p, p' sont incompatibles, d'où le résultat, d'après la CAD.
Donc $\bigcup_{n\in\mathbb{N}} E_n$ est majoré dans Od par un ordinal dénombrable α. F est alors, dans $\mathscr{N}$, une

application de $\mathbb{N}$ dans α, donc sa borne supérieure β est $\leq \alpha$. Donc B est isomorphe à l'ordinal dénombrable β, contrairement à l'hypothèse.

C.Q.F.D.

Un exemple essentiel de CAD

L'ensemble des conditions (c'est-à-dire des individus) est $\mathscr{P}(\mathbb{A}\times\{0,1\})$ où $\mathbb{A}$ est un ensemble qu'on précisera plus loin. On a donc posé $\mathbb{E} = \mathbb{A}\times\{0,1\}$.
On ajoute au langage deux prédicats unaires A_0, A_1 qu'on interprète respectivement dans $\mathscr{M}$ par $\mathbb{A}\times\{0\}$ et $\mathbb{A}\times\{1\}$; et aussi un symbole de fonction unaire i qu'on interprète comme la bijection canonique de $\mathbb{A}\times\{0\}$ sur $\mathbb{A}\times\{1\}$. On a donc les axiomes :
$\forall x(A_0x \leftrightarrow \neg A_1x)$; $\forall x(i(i(x) = x)$; $\forall x(A_0x \rightarrow A_1i(x))$; $\forall x(A_1x \rightarrow A_0i(x))$.

L'ensemble C des conditions non triviales est l'ensemble des parties *finies* de $\mathbb{A}\times\{0,1\}$ *qui sont des fonctions*. Autrement dit, si p est une partie finie de $\mathbb{A}\times\{0,1\}$, on a :
$\mathsf{C}[p] \Leftrightarrow (\forall x \in \mathbb{A})\forall\delta\forall\delta'((x,\delta)\in p, (x,\delta')\in p \rightarrow \delta = \delta')$.

Soient $p, q \in \mathscr{P}(\mathbb{A}\times\{0,1\})$ deux conditions. On pose $p\wedge q = p\cup q$.

Théorème 20. *La CAD est satisfaite.*

Soit $V \subset \mathsf{C}$ une antichaîne dont tous les éléments sont des parties à n éléments de $\mathbb{A}\times\{0,1\}$. On montre, par récurrence sur n, que V *est finie*. C'est évident si $n = 0$. On suppose donc que $n = m+1$ et on choisit $p = \{(a_1,\delta_1),\ldots,(a_n,\delta_n)\} \in V$.
Soit $V_i = \{q \in V$; $(a_i, 1-\delta_i) \in q\}$. On a alors $V = \{p\}\cup V_1\cup\ldots\cup V_n$ et il suffit donc de montrer que V_i est fini pour chaque $i \in \{1,\ldots,n\}$.
Or, si on retire $(a_i, 1-\delta_i)$ à chaque élément de V_i, on obtient une antichaîne à laquelle on peut appliquer l'hypothèse de récurrence.

C.Q.F.D.

Soit $\mathscr{G}$ un générique ; alors $\rho_{\mathscr{G}} = \bigcup_{p\in\mathscr{G}} p$ est une partie de $\mathbb{A}\times\{0,1\}$, qui est une application de $\mathbb{A}$ dans $\{0,1\}$ (*exercice*).
Noter que $\rho_{\mathscr{G}}$ détermine $\mathscr{G}$, puisque $\mathscr{G}$ est l'ensemble des parties finies de $\rho_{\mathscr{G}}$ (*exercice*).

Réels de Cohen

On prend $\mathbb{A} = \mathbb{N}$, donc $\mathbb{E} = \mathbb{N}\times\{0,1\}$; on note que l'ensemble C des conditions non triviales est dénombrable, donc la CAD est évidemment satisfaite, sans même utiliser le théorème 20.

Soit $\mathscr{G}$ un générique ; alors, on a vu que $\rho_{\mathscr{G}} = \bigcup_{p\in\mathscr{G}} p$ est une partie de $\mathbb{N}\times\{0,1\}$, qui est une application de $\mathbb{N}$ dans $\{0,1\}$.
On peut donc considérer $\rho_{\mathscr{G}}$ comme une partie de $\mathbb{N}$, qui est dans $\mathscr{N}$; on l'appelle un *réel de Cohen* sur $\mathscr{M}$.

Lemme 21. *Soit* $D_{\mathscr{G}} = \{p$; $\mathsf{C}[p]$, p *est incompatible avec un élément de* $\mathscr{G}\}$;
alors $D_{\mathscr{G}}$ *est une partie dense de* C.

En effet, si p est une condition non triviale, soit $n \in \mathbb{N}$ tel que $(n,0),(n,1) \notin p$. On a $(n,\delta) \in \rho_{\mathscr{G}}$ et on pose $q = p\cup\{(n,1-\delta)\}$. Alors, on a $\mathsf{C}[q]$, $q \leq p$ et q est incompatible avec $\{(n,\delta)\} \in \mathscr{G}$.

C.Q.F.D.

Théorème 22. *Un réel de Cohen sur $\mathscr{M}$ ne peut être dans $\mathscr{M}$.*

Supposons que $\rho_{\mathscr{G}}$ soit dans $\mathscr{M}$; d'après le lemme 21, $D_{\mathscr{G}}$ est alors une partie dense de C qui est dans $\mathscr{M}$, donc $\mathscr{G} \cap D_{\mathscr{G}} \neq \emptyset$. Soit $p \in \mathscr{G} \cap D_{\mathscr{G}}$; puisque $p \in D_{\mathscr{G}}$, p est incompatible avec un élément de $\mathscr{G}$, ce qui contredit $p \in \mathscr{G}$.

C.Q.F.D.

L'adjonction d'un réel de Cohen permet donc d'obtenir un modèle $\mathscr{N}$ qui contient $\mathscr{M}$, qui a les mêmes individus et *les mêmes bons ordres dénombrables* et qui contient un nouveau réel.

Négation de l'hypothèse du continu

On prend $\mathbb{A} = \mathbb{N} \times \mathbb{B}$; pour chaque $n \in \mathbb{N}$ et $\beta \in \mathbb{B}$, on pose :
$f_\beta(n) = \delta \Leftrightarrow (n, \beta, \delta) \in \mathscr{G}$.
f_β est alors une application de $\mathbb{N}$ dans $\{0,1\}$ c'est-à-dire un réel de $\mathscr{N}$. Donc f est, dans $\mathscr{N}$, une application de $\mathbb{B}$ dans $\mathscr{P}(\mathbb{N})$.

Lemme 23. *f est, dans $\mathscr{N}$, une injection de $\mathbb{B}$ dans $\mathscr{P}(\mathbb{N})$.*

Soient $\beta, \beta' \in \mathbb{B}$, avec $\beta \neq \beta'$. On pose $D = \{p;\ \mathsf{C}[p], (\exists n \in \mathbb{N})((n, \beta, 0) \in p \wedge (n, \beta', 1) \in p)\}$.
Alors D est une partie dense de C, qui est dans $\mathscr{M}$: en effet, si p est une condition non triviale, il suffit de choisir $n \in \mathbb{N}$ qui n'apparait pas dans p et de poser $q = p \cup \{(n, \beta, 0), (n, \beta', 1)\}$.
Il en résulte que $\mathscr{G} \cap D \neq \emptyset$, ce qui montre qu'il existe un entier n tel que $f_\beta(n) = 0$ et $f_{\beta'}(n) = 1$, donc que $f_\beta \neq f_{\beta'}$.

C.Q.F.D.

On rappelle que $P = \mathscr{P}(\mathbb{A} \times \{0,1\})$ est l'ensemble des individus (ou conditions) des modèles $\mathscr{M}$ et $\mathscr{N}$. On a alors :

Lemme 24. *Soient U, V deux parties infinies de P qui sont dans $\mathscr{M}$. S'il existe, dans $\mathscr{N}$, une surjection de U sur V, alors il en existe une dans $\mathscr{M}$.*

Soit F une relation binaire fonctionnelle qui est, dans $\mathscr{N}$, une surjection de U sur V. Il existe donc $p_0 \in \mathscr{G}$ tel que :
$p_0 \Vdash \forall u \forall v \forall w (F(u,v), F(u,w) \rightarrow v = w)$;
$p_0 \Vdash \forall v (V v \rightarrow \exists u \{U u, F(u,v)\})$.
Pour chaque $u \in U$, on pose $E_u = \{v;\ (\exists q \leq p_0)\{\mathsf{C}[q], q \Vdash F(u,v)\}\}$.

- *E_u est dénombrable pour chaque $u \in U$.*

En effet, $u \in U$ étant fixé, on choisit pour chaque $v \in E_u$, une condition $q_v \leq p_0$ telle que $\mathsf{C}[q_v]$ et $q_v \Vdash F(u,v)$. On obtient ainsi une antichaîne dans C :
si $q_v \Vdash F(u,v)$, $q_w \Vdash F(u,w)$ et $v \neq w$, on a $q_v \wedge q_w \Vdash F(u,v), F(u,w), v \neq w$ et aussi $q_v \wedge q_w \Vdash F(u,v), F(u,w) \rightarrow v = w$ puisque $q_v \wedge q_w \leq p_0$. Donc $q_v \wedge q_w \Vdash \perp$, ce qui veut dire que q_v et q_w sont incompatibles.
Or, cette antichaîne est définie dans $\mathscr{M}$, donc est dénombrable. E_u l'est donc aussi puisque, comme on vient de le montrer, l'application $v \mapsto q_v$ est injective.

- $V \subset \bigcup_{u \in U} E_u$.

Soit en effet $v_0 \in V$; on a donc $\mathbf{1} \Vdash V v_0$, donc $p_0 \Vdash \exists u \{U u, F(u, v_0)\}$. Comme $p_0 \in \mathscr{G}$, cette

formule est vraie dans $\mathscr{N}$ et il existe donc $u_0 \in U$ tel que $\mathscr{N} \models F(u_0, v_0)$. Il existe donc $q \in \mathscr{G}, q \leq p_0$ tel que $q \Vdash F(u_0, v_0)$, ce qui montre que $v_0 \in E_{u_0}$.

C.Q.F.D.

On prend maintenant $\mathbb{B} = \mathscr{P}(\mathscr{P}(\mathbb{N}))$. Il existe donc, dans $\mathscr{M}$, deux ensembles $\mathbb{B}_0 \subset \mathbb{B}_1 \subset \mathbb{B}$ où $\mathbb{B}_0$ est dénombrable et $\mathbb{B}_1$ est équipotent à $\mathscr{P}(\mathbb{N})$. Il n'existe, dans $\mathscr{M}$ aucune surjection de $\mathbb{B}_0$ sur $\mathbb{B}_1$, ni de $\mathbb{B}_1$ sur $\mathbb{B}$. Il n'y en a donc pas non plus dans $\mathscr{N}$.
Or, dans $\mathscr{N}$, il existe une injection f de $\mathbb{B}$ dans $\mathscr{P}(\mathbb{N})$. On a donc, dans $\mathscr{N}$ trois sous-ensembles infinis de $\mathscr{P}(\mathbb{N})$: $f(\mathbb{B}_0) \subset f(\mathbb{B}_1) \subset f(\mathbb{B})$ qui sont de cardinaux différents.
L'hypothèse du continu est donc fausse dans $\mathscr{N}$.