Annexe 1

Rappels de logique classique

Nous présentons en annexes de brefs rappels sur les résultats de la logique classique suivis de la présentation d'un certain nombre de voies explorées dans le but, soit d'étendre cette logique, soit de rendre compte de notions telles que la constuctibilité (l'existence d'une solution à un problème n'est assurée que par celle d'un procédé effectif pour sa construction), la connaissance, la compatibilité avec les connaissances actuelles, la vérité dans le passé ou le futur...
Enfin, nous présentons dans les annexes suivantes, deux langages de programmation, Fril inspiré de Prolog raisonne par induction avec des couples (crédibilité, plausibilité), et Mvl également fondé sur Prolog, mais laissant le choix entre plusieurs logiques ; classique, avec défauts ou temporelle.
Pour leur part, les réseaux bayésiens constituent un système rigoureux quoiqu'assez lourd pour formaliser des relations causales.

La logique classique formalise la notion de preuve grâce à une axiomatique précise à l'aide d'axiomes et de règles (aspect syntaxique). Une preuve est aussi appelée une dérivation, c'est à dire une suite de formules dont chacune est soit un axiome soit le résultat de l'application d'une règle sur des axiomes ou des formules antérieures de cette suite.
D'un autre côté, une sémantique est définie par des tables de vérité dans une théorie des "modèles». On a alors le «théorème de complétude» tant pour le calcul propositionnel que pour le calcul des prédicats qui s'exprime par :

F est valide (vrai dans toute réalisation, ce qui s'écrit : $\models$ F)

$\Leftrightarrow$ F est un théorème

(prouvable d'après un système d'axiomes et de règles, noté par $\vdash$ F)

Un troisième aspect (algébrique) est étudié avec les algèbres de Boole et Lindenbaum- Tarski. Nous passerons brièvement en revue les grands axes et résultats en logique et calculabilité dans ce qui suit.

A.1.1. Langage des propositions

Les formules bien formées de la logique propositionnelle du premier ordre sont les mots formés à partir d'un alphabet comportant un ensemble infini V de «variables propositionnelles» (les majuscules A, B,... qui suivent) et des signes dits connecteurs $\{\neg, \vee\}$ de telle sorte que l'on définisse ;
Les formules atomiques sont les éléments de V, puis, si F et F' sont des formules $\neg F$ en est une, $F \vee F'$ également.

On définit la conjonction comme abréviation par : $A \wedge B = \neg(\neg A \vee \neg B)$, l'implication $(A \rightarrow B) = \neg A \vee B$, l'équivalence $A \leftrightarrow B = (A \rightarrow B) \wedge (B \rightarrow A)$ ainsi que l'exclusion réciproque «ou bien» notée $\oplus$ ici par $A \oplus B = (A \wedge \neg B) \vee (\neg A \wedge B)$, et le symbole de Sheffer noté par une barre | avec $A \mid B = \neg(A \wedge B)$.

ASPECT SÉMANTIQUE

Une assignation α est une application (dite valeur de vérité) de l'ensemble des variables propositionnelles V vers {0, 1} appelés «faux» et «vrai», assignation qui s'étend à toutes les formules.
Cette extension est définie par les fameuses tables de vérité à savoir
$\alpha(\neg P) = 1 - \alpha(P)$ pour la négation et :

P	Q	$P \wedge Q$	$P \vee Q$	$P \rightarrow Q$	$P \leftrightarrow Q$	$P \leftarrow Q$	$P \oplus Q$	$P \mid Q$
1	1	1	1	1	1	1	0	0
1	0	0	1	0	0	1	1	1
0	1	0	1	1	0	0	1	1
0	0	0	0	1	1	1	0	1

Les tautologies, sont les formules vraies pour toute assignation (notation $\models F$).
Les premières tautologies du calcul propositionnel sont les 18 suivantes :

Involutivité de la négation $\neg(\neg P) \leftrightarrow P$
Les lois de Morgan, $\neg(P \wedge Q) \leftrightarrow (\neg P \vee \neg Q)$ et $\neg(P \vee Q) \leftrightarrow \neg P \wedge \neg Q$
Les connecteurs $\wedge$ et $\vee$ sont commutatifs :
$P \wedge Q \leftrightarrow Q \wedge P$ et $P \vee Q \leftrightarrow Q \vee P$
Idempotents : $P \wedge P \leftrightarrow P$ $P \vee P \leftrightarrow P$
Associatifs :
$P \wedge (Q \wedge R) \leftrightarrow (P \wedge Q) \wedge R$ et $P \vee (Q \vee R) \leftrightarrow (P \vee Q) \vee R$
Distributivités mutuelles :
$P \wedge (Q \vee R) \leftrightarrow (P \wedge Q) \vee (P \wedge R)$ et $P \vee (Q \wedge R) \leftrightarrow (P \vee Q) \wedge (P \vee R)$
Eléments neutre et absorbant : 0 et 1 désignant respectivement le faux et le vrai, P étant une proposition quelconque :
$0 \wedge P \leftrightarrow 0$ $0 \vee P \leftrightarrow P$ 0 est absorbant pour $\wedge$, et neutre pour $\vee$.
$1 \wedge P \leftrightarrow P$ $1 \vee P \leftrightarrow 1$ 1 est neutre pour $\wedge$, et absorbant pour $\vee$.
Enfin les deux propriétés $P \wedge \neg P \leftrightarrow 0$ et $P \vee \neg P \leftrightarrow 1$ font du calcul propositionnel une algèbre de Boole.

Notons encore la contraposition $(\neg Q \rightarrow \neg P) \leftrightarrow (P \rightarrow Q)$

ASPECT SYNTAXIQUE

Il existe une bonne douzaine d'axiomatiques équivalentes du calcul des propositions, signalons la plus courte, celle de Nicod avec un seul symbole, la barre de Sheffer |, (le «nand» bien connu en informatique), un seul axiome :

$$(A \mid (B \mid C)) \mid ((D \mid (D \mid D)) \mid ((E \mid B) \mid ((A \mid E) \mid (A \mid E))))$$

et une seule règle, le fameux modus-ponens (si A et $A \rightarrow B$, sont connus alors B peut l'être) qui s'énonce dans ce langage : $A, A \mid (B \mid B) \vdash B$.

La négation y est définie par $\neg A = A \mid A$.

Cependant, la syntaxe la plus courante est celle de Hilbert définie sur l'alphabet $V \cup \{\neg, \vee, \wedge, \rightarrow\}$ où V est un ensemble dénombrable de «variables» (ici les majuscules) avec les 10 axiomes :

$A \rightarrow (B \rightarrow A)$ $\quad (A \rightarrow B) \rightarrow (((A \rightarrow (B \rightarrow C)) \rightarrow (A \rightarrow C))$

$A \rightarrow (B \rightarrow (A \wedge B))$ $\quad A \wedge B \rightarrow A$ $\quad A \wedge B \rightarrow B$

$A \rightarrow A \vee B$ $\quad B \rightarrow A \vee B$ $\quad (A \rightarrow B) \rightarrow ((A \rightarrow \neg B) \rightarrow \neg A)$

$(A \rightarrow C) \rightarrow ((B \rightarrow C) \rightarrow (A \vee B \rightarrow C))$

Enfin l'axiome $\neg\neg A \rightarrow A$ (modifié dans l'intuitionnisme) et la règle unique du «modus-ponens» $A, A \rightarrow B \vdash B$.

A.1.2. Langage des predicats

SÉMANTIQUE

Un langage de prédicats est construit sur un alphabet comportant un ensemble dénombrable de variables V, des symboles relationnels (dont éventuellement le symbole d'égalité =), des symboles fonctionnels à 0 places (constantes) 1, 2 ... places, les connecteurs $\{\neg, \vee\}$ et le quantificateur $\exists$ (il existe au moins un).

TERMES Les constantes et variables sont les termes les plus simples. La juxtaposition d'un symbole fonctionnel et de termes séparés (en nombre égal au nombre de places du symbole de fonction), constitue un nouveau terme, c'est-à-dire une expression pouvant être interprétée dans la mesure où les variables le sont.

FORMULES OU PROPOSITIONS

Les propositions «atomiques» sont le «vrai», le «faux», et tous les mots écrits avec un symbole de relation (la plupart du temps binaire) et des termes appartenant aux types sur lesquels portent la relation. Les propositions structurées sont construites à partir des propositions atomiques en les assemblant grâce aux connecteurs logiques comme pour le calcul propositionnel et aux quantificateurs (si F est une formule, $\exists x$ F, en est une).

$\forall$ (quelquesoit) est défini de façon duale par $\forall x\ P(x) = \neg \exists x\ \neg P(x)$.

PROPOSITION CLOSE

Les propositions closes ou «sentences» sont les propositions où toutes les variables y figurant sont «muettes», ou «liées» par un quantificateur ce qui signifie que le sens de la proposition ne change pas si on les remplace par d'autre variables.

ASPECT SÉMANTIQUE

Une réalisation du langage est une application ρ dans une structure M telle qu'à tout symbole fonctionnel est associé une fonction de M dans M avec autant de places (en particulier aux constantes sont associées des éléments de M) et à tout symbole relationnel est associé une relation dans M avec autant de places (en particulier, = est réalisé comme l'égalité). Une assignation α est une application de V dans l'ensemble M, elle se prolonge donc naturellement à tous les termes et par définition elle satisfait une formule si :
A atomique de la forme R t_1 t_2 ... t_n :
$(M, \alpha) \models A$ $\Leftrightarrow$, et $\rho(R)(\alpha(t_1),..., \alpha(t_n))$ est vrai.
Sinon :
$(M, \alpha) \models \neg A$ $\Leftrightarrow$ non $(M, \alpha) \models A$
$(M, \alpha) \models A \vee B \Leftrightarrow (M, \alpha) \models A$ ou $(M, \alpha) \models B$
$(M, \alpha) \models \exists x\, A \Leftrightarrow$ Il existe un c dans M tel que $(M, \alpha(x \leftarrow c)) \models A$ où $\alpha(x \leftarrow c)$ désigne l'assignation donnant la valeur c à x et coïncidant avec α pour les autres variables. On aura donc :
$(M, \alpha) \models \forall x\, A$ $\Leftrightarrow$ Pour tout élément c de M, $(M, \alpha(x \leftarrow c)) \models A$

M est dit modèle de la formule close (notation $M \models F$) si F vraie dans M pour toute assignation, et F est une tautologie valide si elle est vraie dans toute réalisation.

HIÉRARCHIE DES FORMULES

On pose $\Sigma_0 = \Pi_0$ l'ensemble des formules sans quantificateurs (closes ou non) puis $\Sigma_{p+1} = \exists\, \Pi_p$ est défini comme l'ensemble des formules qui (sous forme prénexe, les quantificateurs en premier) s'expriment comme une suite de quantificateurs débutant par $\exists$ et ayant p alternances sur le type de quantificateur, suivie d'une formule sans quantificateurs. $\Pi_{p+1} = \forall\, \Sigma_p$ et $\Delta_p = \Sigma_p \cap \Pi_p$.

ASPECT SYNTAXIQUE

La syntaxe du «calcul des prédicats» de Hilbert est celle du calcul propositionnel où sont ajoutées deux règles de particularisation $[A(x) \rightarrow C] \vdash [\exists\, x\, A(x) \rightarrow C]$ et de généralisation $[C \rightarrow A(x)] \vdash [C \rightarrow \forall x\, A(x)]$ si x non variable libre dans C.

A.1.3. Arithmetique

Une des premières axiomatiques ayant servi à la fondation des mathématiques est celle de Peano (1899) pour l'arithmétique, l'alphabet des symboles utilisés est encore un ensemble dénombrable (au sens naïf) de variables V et les symboles {¬,

$\vee$, $\exists$, 0, S, +, *, =} où S va se réaliser comme la fonction successeur. Les connecteurs $\wedge$ et $\rightarrow$ n'étant que des abréviations.
Les axiomes et règles sont ceux de la logique des prédicats, plus les axiomes de l'égalité et les 6 axiomes dits de Peano :

$\forall x \forall y$ $\quad Sx = Sy \rightarrow x = y$ $\quad x + 0 = x$ $\quad \neg(Sx = 0)$
$\quad x + Sy = S(x + y)$ $\quad x*0 = 0$ $\quad x*Sy = (x*y) + x$

Ainsi que le schéma d'axiome de récurrence (ce n'est pas un axiome, mais une famille infinie d'axiomes), pour toute formule F à une variable libre :

$$[F(0) \wedge \forall x\, F(x) \rightarrow F(Sx)\ ] \rightarrow \forall y\, F(y)$$

On montre que l'arithmétique n'est pas finiment axiomatisable. L'arithmétique du second ordre, elle, considère deux types d'objets (donc deux ensembles de variables), en ce cas, on peut trouver un nombre fini d'axiomes.

Le résultat logique le plus important est que la consistance (ou non-contradiction) de la théorie de l'arithmétique est exprimable dans cette théorie par une formule, mais celle-ci ne peut être ni démontrée, ni réfutée. Cet énoncé de non-contradiction est donc indécidable et montre «l'incomplétude» de l'arithmétique. C'est le célèbre théorème de Gödel (1940) établi grâce à une numérotation de toutes les formules et démonstrations.
Le théorème de Tarski (1944) montre pour sa part qu'il n'existe pas de formule qui puisse assurer de la validité d'un énoncé.

A.1.4. Théorie des ensembles et ensembles flous

Les mêmes résultats subsistent pour la théorie des ensembles de Zermelo-Fraenkel et d'ailleurs toute autre théorie pouvant fonder les mathématiques. La théorie des ensembles est à l'heure actuelle le cadre (plus vaste que l'arithmétique) le plus habituel pour fonder l'ensemble des mathématiques. Il s'agit de définir une structure (plusieurs structures, mais ZF+AC suffit aux mathématiques ordinaires) de graphe (U, =, $\in$) dans laquelle les relations binaires = et $\in$ doivent vérifier les 5 axiomes suivants (avec l'écriture de l'inclusion $x \sqsubset y$ pour $\forall z\ (z \in x \Rightarrow x \in y)$:

AXIOME DE L'UNION
$\forall x \exists y \forall z\ (z \in y \Leftrightarrow \exists t\ z \in t$ et $t \in x)$ $\quad$ y est noté U(x)
AXIOME DES PARTIES
$\forall x \exists y \forall z\ (z \in y \Leftrightarrow z \sqsubset x)$ $\quad$ y est noté P(x)
AXIOME D'EXTENSION $\quad \forall x \forall y \forall z\ (z \in x \Leftrightarrow z \in y) \Rightarrow x = y$
(deux ensembles sont égaux si et seulement si ils ont mêmes éléments)
SCHÉMA D'AXIOME DE SUBSTITUTION
Pour toute relation binaire fonctionnelle F, l'image d'un ensemble est un ensemble
$\forall x \exists y \forall z\ \ z \in y \Leftrightarrow \exists u\ (u \in x$ et $F(u, z))$

On montre alors l'existence d'un élément minimal pour $\in$ (l'ensemble vide $\varnothing$), et l'existence des paires pouvant se former avec deux objets quelconques de U :
$\forall x \forall y \exists z \forall t\ (t \in z \Leftrightarrow (t = x$ ou $t = y))$, z étant noté {x, y}, et on peut définir alors le produit, l'union et intersection, les entiers finis $0 = \varnothing$, $1 = \{\varnothing\}$, $2 = \{\varnothing,\{\varnothing\}\}$, ...,

$n+1 = n \cup \{n\}$. On définit également les ordinaux comme ensembles transitifs (a tel que $\forall x\ \forall y\ (x \in a)$ et $(y \in x) \Rightarrow y \in a)$ où $\in$ est un bon ordre strict.
Cependant, les mathématiques classiques imposent un dernier axiome :

AXIOME DE L'INFINI
$\exists x\ (\varnothing \in x)$ et $\forall y\ (y \in x \Rightarrow y \cup \{y\} \in x)$, il existe un ordinal non fini.
En résumé, il est possible alors de montrer que tous les ordinaux finis forment un ensemble (le «dénombrable" noté ω), et de définir les cardinaux comme ordinaux non équipotents à un ordinal inférieur, $\omega = \aleph_0$ est le premier cardinal infini.

Cette axiomatique ZF n'est pas finiment axiomatisable à cause du schéma de substitution, les résultats de Gödel et de Tarski sont encore valable dans ZF et ses prolongements. A partir de sa consistance (l'existence d'une telle structure) on peut montrer l'existence d'univers parallèles tels que ZF + AF, ZF + AC, ZF + HGC, ou bien ZF + ¬AF, ZF + ¬AC, ZF + ¬HGC, pour citer les énoncés les plus connus avec :

AXIOME DE FONDATION AF : $\forall x \neq \varnothing\ \exists y \in x\ (x \cap y = \varnothing)$, en particulier il n'y a pas d'atome (c'est à dire d'ensemble a vérifiant $a = \{a\}$)

AXIOME DU CHOIX AC : Sur tout ensemble il existe au moins un bon ordre, ce qui fait que tout ensemble est en bijection avec un cardinal (une douzaine d'énoncés importants sont équivalents à AC, notamment celui de Zorn dont il est question à l'annexe 4).

HYPOTHÈSE DU CONTINU (généralisée) HGC : Le cardinal infini $\aleph_{\alpha+1}$ suivant $\aleph_\alpha$ est celui de $P(\aleph_\alpha)$, c'est une conséquence de AF et l'axiome de constructibilité (tout ensemble est définissable par une formule à une variable libre), par ailleurs, il est prouvé que HGC entraîne AC.
D'autres théories permettent de fonder les mathématiques, ainsi celle de Gödel-Bernays dont on peut montrer l'équivalence avec ZF. Dans cette théorie il existe un symbole supplémentaire de prédicat unaire M (M(x) sera interprété par «x est un ensemble»).

AXIOMATIQUE DE ZERMELO

C'est la structure moins forte $(U, =, \in)$ munie des axiomes d'extensionalité, de la paire : $[\forall x\ \forall y\ \exists z\ \forall t\ (t \in z \Leftrightarrow t = x$ ou $t = y]$, z étant noté $\{x, y\}$), de l'union, des parties et du schéma d'axiome de compréhension : pour toute formule à une seule variable libre A (donc éventuellement paramétrée par des constantes)
$[\forall x\ \exists y\ \forall z\ (z \in y \Leftrightarrow z \in x$ et $A(z))]$, y étant noté $y = \{z \in x / A(z)\}$.
Cette axiomatique permet de définir les opérations ensemblistes usuelles et les ordinaux, mais pas les cardinaux. La meilleure introduction en théorie des ensembles se trouve dans [Krivine 72].

THÉORIE AXIOMATIQUE DES ENSEMBLES FLOUS

Plusieurs axiomatiques de la logique floue (avec une infinité de valeurs ont été réalisées [Pavelka 79], mais nous présentons un point de vue plus original. Une

théorie du second ordre introduite par [De Glas 84] formalise la théorie des ensembles flous. Il est nécessaire d'avoir une classe V de variables (les ensembles) et une autre (notées par des lettres grecques, les degrés), le symbole d'égalité, un symbole d'ordre < pour les degrés et un symbole de relation ternaire noté $\in$, (on notera $x \in_\alpha y$ et on lira «x appartient à y avec le degré α»). Les 12 axiomes sont :

1 Extensionalité : $\forall x\ \forall y\ \forall z\ \forall\alpha\ (z \in_\alpha x \Leftrightarrow z \in_\alpha y) \Rightarrow x = y$

2 L'appartenance est une fonction $\forall x\ \forall y\ \forall\alpha\ \forall\beta\ (x \in_\alpha y \wedge x \in_\beta y) \Rightarrow \alpha = \beta$

3 Les degrés forment un ordre total avec extrémités,
on pose $D(\alpha) = \exists x\ \exists y\ (x \in_\alpha y)$ qui signifie «être un degré» :

$\forall\alpha\ \forall\beta\ \forall\gamma\ [(\alpha < \beta \Rightarrow D(\alpha) \wedge D(\beta)) \wedge (D(\alpha) \Rightarrow \alpha < \alpha) \wedge (D(\alpha) \wedge D(\beta) \wedge D(\gamma) \wedge \alpha < \beta \wedge \beta < \gamma \Rightarrow \alpha < \gamma) \wedge (D(\alpha) \wedge D(\beta) \wedge \alpha < \beta \wedge \beta < \alpha \Rightarrow \alpha = \beta) \wedge (D(\alpha) \wedge D(\beta) \Rightarrow \alpha < \beta \vee \beta < \alpha) \wedge (\exists 0\ \exists 1\ \forall\alpha\ D(0) \wedge D(1) \wedge (D(\alpha) \Rightarrow 0 < \alpha \wedge \alpha < 1)]$

On prend les définitions :

$E(x) = (\forall y\ \forall\alpha\ (y \in_\alpha x) \Rightarrow \alpha = 0 \vee \alpha = 1)$ pour «être un ensemble exact»

et pour l'inclusion : $(x \sqsubset y) = \forall z\ \forall\alpha\ (z \in_\alpha x \Rightarrow \exists\beta\ \ \beta < \alpha \wedge z \in_\beta y)$

4 Axiome de la paire : $\forall x\ \forall y\ \forall z\ \exists p\ (E(p) \wedge (z \in_1 x \Leftrightarrow z = x \vee z = y))$

p sera noté {x, y} y compris pour des degrés et un couple (x, y) est par définition, comme dans la théorie classique des ensembles, {x, {x, y}}.

5 Existence de degrés complémentaires

$\exists c\ [\forall x\ \exists\alpha\ \exists\beta\ (E(c) \wedge (x \in_1 c \Leftrightarrow D(\alpha) \wedge D(\beta) \wedge x = (\alpha, \beta))$

$\wedge\ \forall\alpha\ \forall\beta\ \forall\gamma\ ((\alpha, \beta) \in_1 c \Rightarrow (\beta, \alpha) \in_1 c) \wedge$

$[(\alpha, \beta) \in_1 c \wedge (\alpha, \gamma) \in_1 c \Rightarrow \beta = \gamma))]$

$\wedge\ \forall\alpha\ \forall\beta\ \forall\alpha'\ \forall\beta'\ (\alpha, \beta) \in_1 c \wedge (\alpha', \beta') \in_1 c \wedge (\alpha < \alpha') \Rightarrow \beta' < \beta)$

Cet ensemble c est l'ensemble des «couples complémentaires», on peut alors noter $\neg\alpha$ pour β si $(\alpha, \beta) \in_1 c$.

6 Axiome du complémentaire (x' sera noté $\neg x$) $\forall x\ \ \exists x'\ \forall y\ (y \in_\alpha x) \Rightarrow (y \in_{\neg\alpha} x')$

On montre alors que $\forall x\ \forall y\ \forall\alpha\ (y \in_{\neg\alpha} x \Leftrightarrow y \in_\alpha \neg x)$

7 Axiome de l'α-coupe $\forall x\ \forall\alpha\ \forall\beta\ \exists! y\ \forall z\ (E(y) \wedge (\alpha < \beta \wedge z \in_\beta x \Leftrightarrow z \in_1 y))$

On note $\gamma = \max(\alpha, \beta)$ la formule $D(\gamma) \wedge (\alpha < \beta \Rightarrow \gamma = \beta) \wedge (\beta < \alpha \Rightarrow \gamma = \alpha)$

8 Axiome de l'union (r noté U(x)) :

$\forall x\ \exists r\ \forall y\ \forall\gamma\ (y \in_\gamma r \Leftrightarrow \exists z\ \exists\alpha\ \exists\beta\ y \in_\alpha z \wedge z \in_\beta x \wedge \gamma = \max(\alpha, \beta))$

9 Axiome des parties : $\forall x\ \forall y\ \exists p\ (E(p) \wedge (y \in_1 p \Leftrightarrow y \sqsubset x)$

10 Axiome de fondation : $\forall x\ \forall\alpha \neq 0\ \neg(x \in_\alpha x)$

11 Axiome de l'infini :

$\exists x\ (\exists y\ \exists\alpha \neq 0\ y \in_\alpha x) \wedge \forall y\ \forall\alpha\ (y \in_\alpha x) \Rightarrow \exists\beta\ U(\{y, \{y\}\}) \in_\beta x$

12 Schéma d'axiome de substitution

Soient F et G deux formules avec au moins deux variables libres, alors :

$\forall a\ \forall b\ \forall x\ \forall y\ \forall y'\ [(F(x, y, a) \wedge F(x, y', a) \Rightarrow y = y')$

$\wedge\ \forall\alpha\ \forall\beta\ (G(y, \alpha, b) \wedge G(y, \beta, b) \Rightarrow D(\alpha) \wedge \alpha = \beta)]$

$\Rightarrow \forall z\ \exists t$ (appelé image de x par F)

$\forall y\ \forall\alpha\ (y \in_\alpha t) \Leftrightarrow \exists x\ \exists\beta\ \alpha < \beta \wedge (z \in_\beta x) \wedge F(x, y, a) \wedge G(y, \alpha, b)$

Avec ces axiomes, il est possible de définir l'union et l'intersection en prouvant qu'il s'agit bien d'opération correspondant respectivement aux max et min avec toutes les propriétés usuelles de treillis distributif complémenté ainsi que les lois de Morgan

évoquées au chapitre I, et enfin de prouver l'existence de l'ensemble vide. On montre que cette axiomatique est consistante relativement à ZF.

A.1.5. La Récursivité

Toutes les notions suivantes sont définies sur N et les produits cartésiens N^p, des définitions analogues peuvent être faites dans la théorie plus vaste des ensembles avec les mêmes résultats.

LES FONCTIONS ÉLÉMENTAIRES sont définies comme le plus petit ensemble de fonctions contenant la fonction constante zéro, la fonction successeur, les projections, l'addition, la multiplication, la quasi-différence définie par $x \div y$ = [si ($x \leq y$) alors $x - y$ sinon 0], et stable par sommation, produit et composition.
On peut montrer alors que ces fonctions sont exactement celles qui sont PL_2-calculables par programmes comprenant 0, «entrée», «sortie», «incrémentation», «boucle simple répéter n fois», et limités à 2 boucles imbriquées.

LES FONCTIONS PRIMITIVES RÉCURSIVES sont une classe F_{RP} plus vaste de fonctions constituée par le plus petit ensemble de fonctions contenant la constante zéro, la fonction successeur, les projections, et stable par composition et récurrence simple.
Une autre identification de F_{RP} est l'ensemble des fonctions PL-calculables par programme comprenant 0, «successeur», «entrée», «sortie», «affectation», «test», «boucle», mais pas le débranchement «goto».
Un ensemble de N^p (un prédicat) est récursif primitif, si par définition, sa fonction caractéristique est récursive primitive.

UN PRÉDICAT (OU PARTIE DE N^p) EST RÉCURSIVEMENT ÉNUMÉRABLE (semi-décidable) s'il est la projection d'un ensemble récursif primitif. Il s'agit en fait du plus petit ensemble de parties contenant {1}, les graphes de l'addition et de la multiplication, et stable par changement de places, union, intersection, quantification existencielle et quantification universelle bornée. C'est l'ensemble des objets définissables par les formules $\sum_1$ de la hiérarchie arithmétique des formules, et également l'ensemble des prédicats reconnus par automate de Turing (A est semi-décidable si l'automate reconnait les énoncés $x \in A$, mais pas ceux du type $x \notin A$). Les ensembles récursivement énumérables ont également 5 autres identifications par différentes familles de systèmes de règles tel que système de Post.

LES FONCTIONS RÉCURSIVES (calculables) sont le plus petit ensemble de fonctions contenant zéro, la fonction successeur, les projections et stable par composition, récurrence et minimisation, c'est aussi l'ensemble des fonctions dont le graphe est récursivement énumérable (F_{RP} est énumérable dans F_R).
Les fonctions récursives sont également identifiées suivant quatre autres points de vue : les fonctions Turing-calculables, Markov-calculables, PLD-calculables et les fonctions représentables dans le λ-calcul :

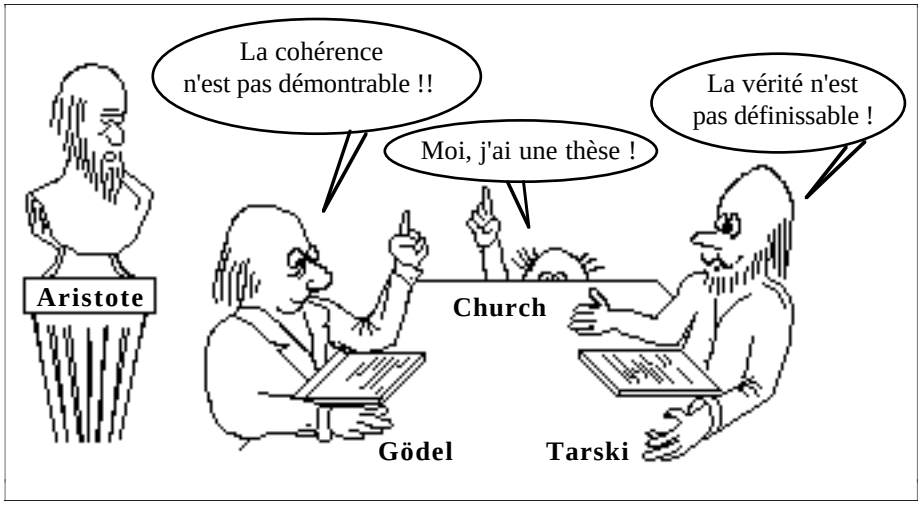
UN AUTOMATE DE TURING est un quintuplet (A, Q, {G, S, D}, P) où A est un alphabet fini, par exemple deux signes {0, 1}, Q un ensemble fini «d'états» comportant notamment l'état initial q_0 et l'état final q_1, et P le «programme» constitué par une fonction partielle de A*Q dans A*{G, S, D}*Q.
Un calcul à partir d'un mot u de A* (ensemble des suites finies d'éléments de A) est alors une suite de «descriptions» notée $q_0u \vdash, \ldots, \vdash (v, q_1)$ telle qu'à chaque étape on ait, dès lors que P(a, q) = (a', M, q'), (u ou v pouvant être vides) uqav $\vdash$ uq'a'v au cas où M = S, uqav $\vdash$ u'q'fa'v si M = G et u = u'f avec f $\in$ A et enfin uqav $\vdash$ ua'q'v si M = D. Le calcul s'arrête dès que q' est l'état final.
Une fonction f est T-calculable si pour l'écriture binaire de x, elle s'arrête sur l'état final pour la valeur binaire de f(x) et ne s'arrête pas si f(x) n'est pas défini.

UNE GRAMMAIRE DE MARKOV sur l'alphabet A = {0, 1} est la donnée d'un alphabet auxiliaire B et d'une liste P de règles de «production» de couples (u, u') dans (A $\cup$ B)*. Une dérivation à partir d'un mot de A* (ensemble des suites finies d'éléments de A) est une suite de mots telle qu'à chaque étape la première production applicable dans la lecture gauche à droite, fasse passer au mot suivant. Une fonction f est alors dite M-calculable s'il existe une grammaire de Markov telle que pour tout x en représentation binaire, il y a une dérivation débutant en x et se terminant en f(x), ou ne terminant pas si f(x) n'est pas défini. Une fonction est PLD-calculable si elle se calcule par programme comprenant 0, «successeur», «entrée», «sortie», «affectation», «test», «boucle», et le débranchement «goto».

REPRÉSENTABILITÉ EN Λ-CALCUL
Le λ-calcul est le plus petit ensemble de termes contenant un ensemble dénombrable de variables et stable par «l'application» (uv) si u et v sont des termes, et par "l'abstraction» λx t où x est une variable et t un terme. On définit une α–équivalence des termes λx u et λx'u' dans la mesure où u' est équivalent à u dans lequel x' est substitué à toutes les occurences de x (ils ne diffèrent que par des changements de nom des variables). Λ est l'ensemble quotient.
La β-réduction consiste à déduire d'un terme, un terme sans «rédex» c'est à dire sans sous-terme de la forme (λx u)t, terme que l'on remplace par u[où t prend la place de x]. Celà signifie concrètement que l'on applique la fonction u de variable x au terme t. La forme normale (sans rédex) est unique dans Λ.
On pose I = λx x (l'identité) et F = λx λy y (le faux ou zéro), K = V = λx λy x (le vrai), ensuite peuvent être définis la condition IF = λb λx λy b x y, puis la négation $\neg$ = λx (IF x F V), les connecteurs ET = λx λy x y F, OU = λx λy x V y, enfin les entiers de Church :
$\underline{0}$ = F, $\underline{1}$ = λf λx (f x), $\underline{2}$ = λf λx (f (f x)) et $\underline{n}$ = λf λx (f^k x).
On dit alors que la fonction f de N^n dans N est représentable en λ-calcul par F si et seulement si pour tous entiers k_1, ..., k_n si f(k_1, ..., k_n) n'est pas défini alors l'expression F$\underline{k}_1$, ..., $\underline{k}_n$ n'est pas réductible sinon si f(k_1, ..., k_n) = k alors l'expression F $\underline{k}_1$, ..., $\underline{k}_n$ se réduit en $\underline{k}$.
On peut en effet construire toutes les fonctions récursives telles que :
SUC = λn λf λx ((n f) (f x)), la somme + = λn λm λf λx ((n f) ((m f) x)) et le produit * = λn λm λf λx ((n (m f)) x).

UN ENSEMBLE EST RÉCURSIF (décidable) si sa fonction caractéristique est récursive, cela revient au même de dire qu'il est récursivement énumérable ainsi que son complémentaire. Ce sont les ensembles $P_R = \Delta_0$ définissables par une formule sans quantificateur. On montre que P_{RE} est auto-énumérable et que l'on a les inclusions strictes $P_{RP} \sqsubset P_R \sqsubset P_{RE}$.

D'autres notions ont été élaborées dans le but de formaliser la notion "d'ensemble aléatoire», ainsi un ensemble est «inaproximable» s'il est infini et ne contient aucun ensemble infini récursivement énumérable.
Un automate de Turing qui peut être assimilé à la suite finie des instructions de son programme P, est donc (codé en binaire) assimilé à un entier k de taille m (m bits). Or, pour une taille m donnée, la probabilité pour un automate de Turing de taille m de s'arrêter sur k à partir d'une donnée vide, est $1 / 2^m$. Pour tout entier n, on pose H(n) la complexité de Chaitin-Kolmogorov, comme la taille du plus petit programme s'arrêtant sur n. Le nombre de Chaitin Ω est défini comme la probabilité qu'un automate de Turing s'arrête, donc $\Omega = \sum_{(n \in N)} 1/2^{H(n)}$. On montre que ce réel, (ce qui revient au même, cette suite binaire, ou cet ensemble d'entiers) est définissable dans $\Delta_2 - (\Sigma_1 \cup \prod_1)$ et qu'il est incompressible [Delahaye 94].
Un ensemble A est dit aléatoire ou "incompressible» s'il existe un entier c tel que pour tout programme p, les énoncés $n \in A$ ou leur négation qui sont reconnus par p sont en nombre inférieur à H(p) + c.
Enfin, au second ordre, les problèmes résolus en temps polynômial par une machine de Turing non déterministe (NP) sont ceux qui sont définis au second ordre par une formule $\Sigma_1{}^1$, c'est à dire quantifiée existenciellement sur des relations suivi par une formule du premier ordre.



La thèse de Church n'est pas un énoncé mathématique, mais l'assertion suivant laquelle, jusqu'à preuve du contraire, les fonctions récursives sont les fonctions «effectivement calculables dans la pratique».
Il existe des extensions de la logique classique telles que les langages infinis (conjonctions infinies ou quantifications infinies) et la logique du second ordre (quantification sur des relations par exemple).