Une histoire de la logique mathématique, de la philosophie à l'informatique

Christian Retoré

LIRMM Univ Montpellier

La logique est elle sulfureuse?

Lucifero: "Forse tu non pensavi ch'io LOICO fossi.
Dante Alighieri (1265-1321) Comedia, Inferno XXVII

Une traduction pourrait être:

Lucifer: « *Sans doute ne savais-tu pas que j'étais aussi bon logicien.* »

Il y eut des tensions entre les logiciens et les autorités religieuses
(Abélard, Avicenne,… les aristotéliciens du Moyen-Âge, Platon « passait » mieux)

Parcours

Formation:

- *Maitrise maths pures U. Paris 6 - 1986*
- *DEA et thèse maths U. Paris 7 - 1993 (dir. J.-Y. Girard)*
- *HDR informatique U. Nantes - 2002*

Emplois:

- Allocataire MESR 1987-1989
- Research assistant Imperial College 1989-1991
- ATER 25e Angers 1991-1993
- INRIA
  - Postdoc G. Berry Sophia-Antipolis
  - Chargé de Recherche Nancy Rennes Nantes Bordeaux 1994-2003
  - Responsable équipe projet SIGNES Bordeaux 2002-2011
- Univ Bordeaux LaBRI prof 2003-2014
- Univ Montpellier LIRMM 2014→ …

Avant la logique « moderne »

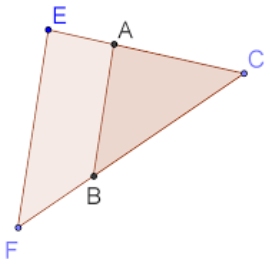
Aristote

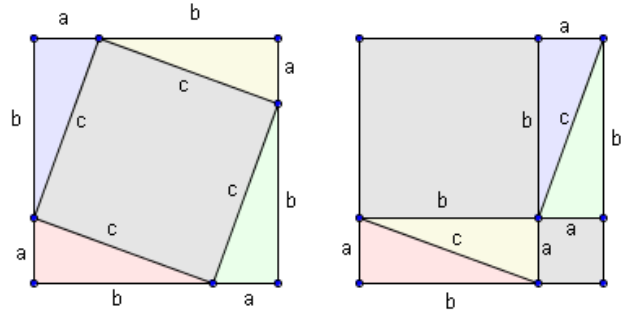
L'antiquité après Aristote

Le Moyen-Âge et la scolastique

La logique algébrique (XVIIe XVIIIe XIXe)

La logique





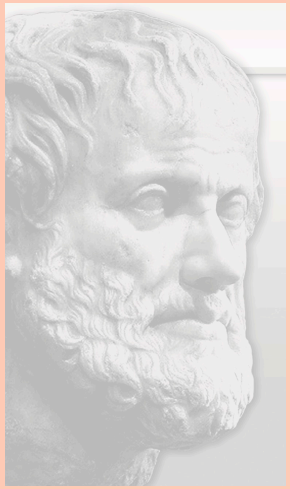
- Art de raisonner correctement
- Avec la rigueur des raisonnements mathématiques (Thalès, Pythagore,… VIIe siècle av. J.C)
- Dériver correctement des énoncés

  …mais à partir de quels axiomes avec quelles règles?
- Bien plus tard (fin XIX^{e}) étude de la vérité dans des situations particulières (modèles), lien entre ces situations.
- À étudier en premier.

« Celui qui souhaite atteindre la perfection humaine
doit d'abord étudier la logique,
puis les diverses branches des mathématiques
dans l'ordre qui convient,
puis la physique et enfin la métaphysique. »
(Maimonides, XIIe)

Aristote (III av JC) & la scolastique (Moyen-Âge)

- Certains types d'énoncés:
  - A Tout A est B
  - E Certains A sont B
  - I Aucun A est B
  - O Tous les A ne sont pas B.
    (ou Certains A ne sont pas B,
    mais le **thème** est différent)
- Baroco :
  - *tout P est M,*
  - *or quelque S n'est pas M,*
  - *donc quelque S n'est pas P*



Principes (Aristote, Avicenne)

Avicenne ibn Sina (980-1037)

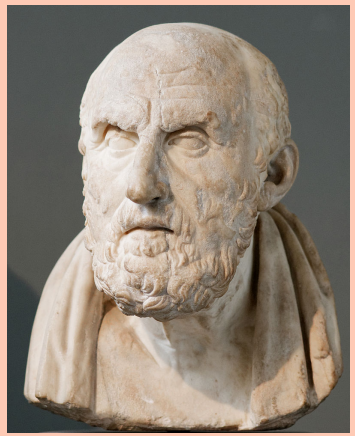
- Identité:
  - Tout A est A
- Non contradiction: pour tout énoncé G
  - NON (G et NON G)
- Tiers exclus **(tertium non datur)** : pour tout énoncé G:
  - (G ou NON G)

"Tout personne niant le principe de non contradiction devrait être battue et brûlée jusqu'à ce qu'elle admette qu'être battu n'est pas la même chose que ne pas être battu, et qu'être brulé n'est pas la même chose que ne pas être brûlé" Avicenne (980-1037) en réponse à des religieux souhaitant accommoder ce principe.

Règles (Stoïciens)

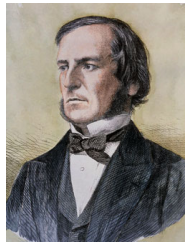
- Stoïciens: règles propositionnelles
- **Modus ponens:**
  - Si A alors B
  - Or A
  - Donc B.
- **Modus tollens:**
  - Si A alors B.
  - Or NON B.
  - Donc NON A.
- **Ex falso quodlibet sequitur :**
  du faux déduit ce qui te plait

Chrysippe de Soles
logicien stoïcien
(280—206 av. JC, Anatolie).



Logique algébrique: XIX^{e} Angleterre États-Unis
Leibnitz et ses successeurs Boole, De Morgan, Pierce

- Précurseur: Leibniz (1646-1716)
- Lois et calculs
- Calcul propositionnel: tables de vérité



- Pour les prédicats des règles parfois fausses
  $\forall x[I(x) -> (F(x) \vee M(x))]$
  $\Leftrightarrow$
  $\forall x(I(x) -> F(x))$ ou
  $\forall x(I(x) -> M(x))$
  pensez à
  I=Individu
  F= femme
  M=homme …

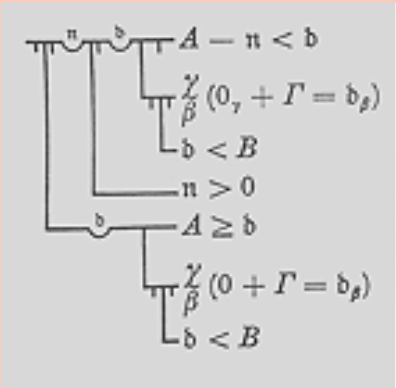
Le XXe siècle

Les débuts de la logique mathématique

La logique du premier ordre

Calcul des prédicats (formules quantifiées)
Gottlob Frege (1848-1925)
David Hilbert (1862-1943),

- Formules avec des variables,
- Sur lesquelles on peut quantifier
- Incluent strictement les énoncés A E I O d'Aristote
- *Tout entier est la somme de quatre carrés:*
  pour tout n il existe a b c et d tels que $n=a^2+b^2+c^2+d^2$
- Idéographie: notation pour les formules et les preuves (à mon avis: illisible, voir ci-contre)



Règles de déduction avec quantificateurs
David Hilbert (1862-1943), Jacques Herbrand (1908-1931)

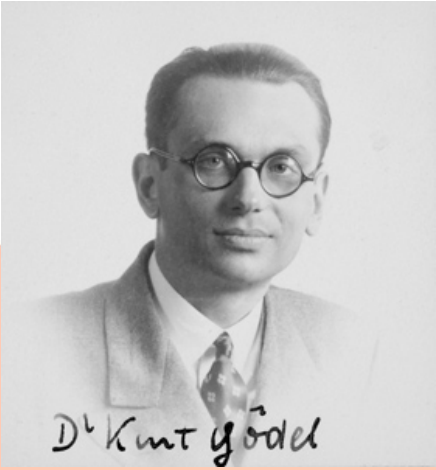
- SI on a établi P(x) (sans rien supposer sur x)
  ALORS on a ∀x P(x) sous les mêmes hypothèses
  (règle de généralisation ou d'abstraction
  formalisation de Aristote)
- SI on a établit ∀x P(x)
  ALORS on a P(t) pour tout terme particulier

Herbrand à 23 ans, peu avant son fatal accident d'alpinisme.

Calcul des prédicats: vérité dans un modèle
Leopold Löwenheim (1878-1957)

- La même chose, en plus compliqué:
  - Ensemble (domaine) par exemple les gens, les nombres,…
  - Interprétation des constantes, des relations, …
    - Dort: ensemble de personnes
    - Connaît: ensemble de couples de personnes
    - $n \leq p$
    - $n=p+q$
  - On peut vérifier dans un modèle donné que, par exemple:
    - Pour tout x il existe y, x connaît y et y dort;
    - Pour tout n pour tout p, $n \leq p+n$

Complétude du calcul des prédicats



- Validité: Toute formule démontrable formellement est vraie dans tout modèle,.
- **Complétude (Gödel, 1929) :**
  Toute formule vraie dans tout modèle est formellement démontrable:
  ce résultat relie les deux notions de vérité, vérité dans les modèles et prouvabilité.

Cet énoncé dont la signification était peu claire à l'époque découle aussi des travaux de 1923 de Thoralf Skolem (1887-1963), ci-contre, comme Gödel l'avait remarqué.

Un drôle de personnage, mort de faim par crainte d'être empoisonné. Mais aussi un génie auteur de plusieurs théorème clés de la logique athématique, et il inventa la première notion de calculabilité et par là même il est à l'origine de l'informatique.

De la logique à l'informatique (merci à Hilbert et à Gödel!)

Les ordinateurs sont issus de la notion de calculabilité et non l'inverse.

Conservativité & cohérence (Hilbert)

Paradoxe de Russell
$U = \{X / X \notin X\}$
$U \in U$?
$U \notin U$?

- Soient
  - une théorie simple R (une théorie dont on ne doute pas)
    par ex. l'arithmétique
  - une théorie I plus complexe que R (on doute de la cohérence de I)
    par ex. l'analyse ou la théorie des ensembles ou …
- CONSERVATIVITÉ: pas plus de résultats sur R en passant par I que directement.
  - Par ex avec les réels on n'obtiendra pas 0=1
  - Autre ex: pour x,y,z entiers >0, n>2
    $x^n+y^n \neq z^n$ (grand th de Fermat, Wiles 1994)
    avec de l'analyse complexe, de l'algèbre commutative
    opeut-on le faire dans l'arithmétique ????????
- COHÉRENCE: montrer en raisonnant sur les preuves formelle (qui sont finies) qu'une contradiction dans I entrainerait une contradiction dans R qui est sans contradiction

Gödel met fin aux espoirs de Hilbert

- Premier théorème d'incomplétude (Gödel 1930):
  Soit T une théorie (cohérente) contenant l'arithmétique,
  alors il existe une formule F (qui affirme sa non prouvabilité)
  telle que T |-/- F et T |-/- ~F
- Second théorème d'incomplétude (Gödel 1930):
  Soit T une théorie (cohérente) contenant l'arithmétique,
  alors T ne démontre pas la cohérence de T
- Conservativité et cohérence ne seront jamais établies
  Contre l'intuition de tous les grands mathématiciens de son temps.

Hilbert + Gödel → calculabilité

- Mécanisation du raisonnement → décidabilité
- Fonctions primitives récursives
- Idée:
  - Formules finies
  - Preuves finies
  - Codage par des entiers
  - En raisonnant / calculant sur les entiers on montre la cohérence via un codage:
    - $Pr_T(d,a)$: d est le code d'une démonstration de la formule codée par a.
    - Cohérence: $\neg(\exists d\ PR_T(d,\langle 0=1\rangle))$

Gödel introduit les deux ingrédients clés de l'INFORMATIQUE:

1. La calculabilité
2. Le codage on peut représenter des données, même structurées par des entiers. Le codage et le décodage se calculent.

Gödel → Church →Turing - - - - > ordinateur

- Gödel: Vienne -> Princeton Church dès 1934
- Turing ingénieur venu étudier auprès de Church 1937/38
  S'oriente vers un modèle de calcul plus proche des machines et circuits
- Kleene montre en 1936 que les 3 notions suivantes coïncident:
  - Lambda calculable (autre notion due à Church)
  - Calculable par une machine de Turing (perfectionné par von Neuman)

  En ramenant les deux notions à:
  - Défini par une fonction récursive de Gödel Herbrand
- Cette notion de calculable (ou pas) reste la même avec les ordinateurs quantiques — même si cette nouveauté est intéressante « en moyenne » du point de vue de la complexité par ex. pour les problèmes NP.

Une application classique de la logique mais pertinente pour MUSE: sureté matérielle et logicielle, notamment embarqués

La logique peut-elle aider à soigner plus sûrement ?

Sûreté des applications critiques

- Des enjeux vitaux ou financiers, par ex:
  - Robotique chirurgicale
  - Logiciel embarqué, circuits (aéronautique)
  - Protocoles cryptographiques de connexion et d'authentification (banque, police, armée,…)
- Deux techniques sures, toutes deux logiques:
  - Vérification: on prouve formellement les propriétés du logicielles (logique classique, logiques modales, temporelles, logique de Hoare ou de séparation)
  - Extraction de programme certifiés

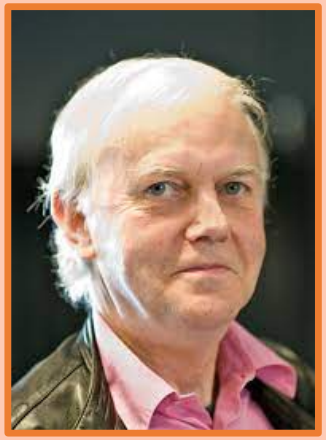
Programme certifiés

- **Procédure:**
  1. On écrit la spécification du programme: (équations) qui calcule une fonction F de A dans B
  2. On démontre formellement en logique intuitionniste que
     - pour tout x de type A
     - il existe un y de type B
     - tel que P(x,y)
       en utilisant les règles de la logique et les équations
  3. La preuve formelle est un programme qui calcule F(X) pour X:A
- **Le programme obtenu (lent mais 100% sûr) fait exactement ce qu'il est supposé faire.**

Si ce programme F vérifie la correction d'un schéma de circuit ou un autre programme, la lenteur n'est pas forcément un problème: on fait tourner F UNE seule fois.

Mes parents logiques

- Jean-Yves Girard (né en 1947) <- Kreisel <- Gödel
  médaille d'argent CNRS 1983
  Calcul avec des preuves pour les logiques d'ordre omega
  preuves et ordinaux
  sémantique dénotationnelle
  logique linéaire micro programmation
  mon directeur de thèse



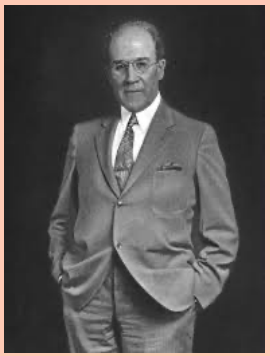
- Gérard Huet (né en 1947)
  membre de l'institut / prix Herbrand 1998 / grand prix INRIA 2011
  Calcul des constructions et démonstrateur Coq
  Programmation fonctionnelle CaML
  Plateforme pour l'analyse du Sanskrit
  (automates sophistiqués en CaML)
  guide et soutien pour la création de l'équipe INRIA « signes linguistique, grammaire et sens » à Bordeaux
  rapporteur HDR

Correspondance logique ⇔ calcul (Curry-Howard)

LOGIQUE	INFORMATIQUE
FORMULE A	TYPE A
PREUVE D DE A	PROGRAMME D DE TYPE A
NOMALISATION DE LA PREUVE D Remplacement des hypothèses par leur preuve	EVALUATION DU PROPGRAMME D Remplacement des variables par leur valeur

Logique linéaire (plus perso)

- Représentation des preuves par des graphes (réseaux de démonstration)
- Evaluation en parallèle des différents calculs contenus dans une preuve
- Quelles fonctions sont ainsi calculables?
- sémantique dénotationelle:
  - types ~ sortes espaces topologiques points et « ouverts » dénombrables
- - fonctions calculables ~ fonctions continues



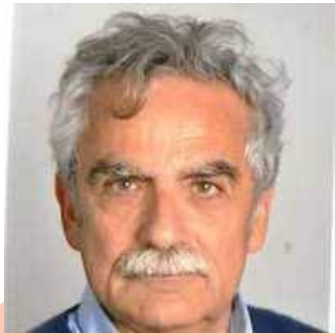
Une application « muse »: sémantique du langage naturel et aide au diagnostic de pathologies mentales

La logique peut-elle aider à établir un diagnostic psy?

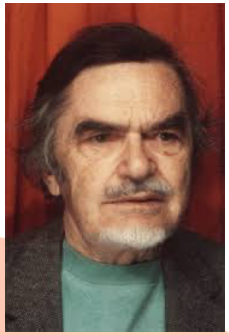
L'application au diagnostic est due à Maxime AMBLARD
(U. Lorraine Sémagramme LORIA – ancien doctorant de Bordeaux)
→ Projet ODiM - Outils informatisés d'aide au Diagnostic des Maladies mentales Action Exploratoire Inria
→ Projet MePheSTO Digital Phenotyping 4 Psychiatric Disorders from Social Interaction Projet Inria-DFKI

Analyse de la structure logique de discours ou de dialogue

- Sujet perso:
  phrase → analyse à la Lambek → Formule logique (DRS)
  DRS= formule logique + référents de discours (pour les pronoms)
  Phrase → DRS par ex. plateforme Grail (Moot, LIRMM)
- Discours? Relations discursives entre DRS (Asher)
  (relation entre formules logiques: logique d'ordre supérieur)
  - élaboration;
  - conséquence;
  - succession narrative;…
- Objectif standard: analyse automatique de texte
  y compris de leur structure logique:
  qu'est ce qui est affirmé, réfuté, affirmé sous conditions, …



Alain Lecomte
(né en 1947)



Joachim Lambek
(1922-2014)

Nicholas Asher IRIT (Toulouse)
(né en 1954)
Médaille d'argent CNRS 2019

Dialogue Patient Psychologue

B_{124} Oh ouais et pis compliqué et c'est vraiment très très compliqué la politique c'est quelque chose quand on s'en occupe faut être gagnant parce qu'autrement quand on est perdant c'est fini quoi

A_{125} Oui

B_{126} J. C. D. est mort, L. est mort, P. est mort euh (...)

A_{127} Ils sont morts parce qu'ils ont perdu à votre avis

B_{128} Non ils gagnaient mais si ils sont morts, c'est la maladie quoi c'est c'est

A_{129} Ouais c'est parce qu'ils étaient malades, c'est pas parce qu'ils faisaient de la politique

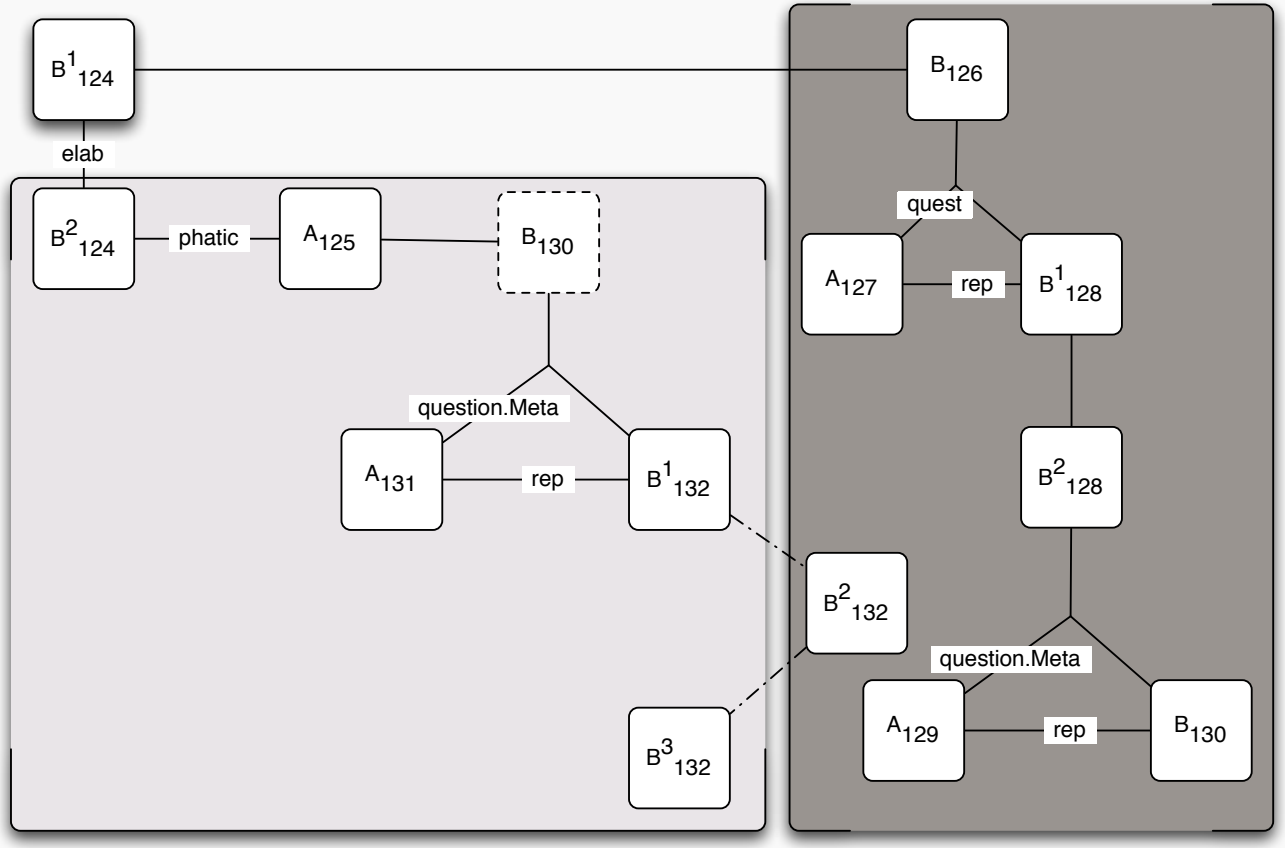
B_{130} Si enfin

A_{131} Si vous pensez que c'est parce qu'ils faisaient de la politique

B_{132} Oui tiens oui il y a aussi C. qui a accompli un meurtre là il était présent lui aussi qui est à B. mais enfin c'est encore à cause de la politique ça

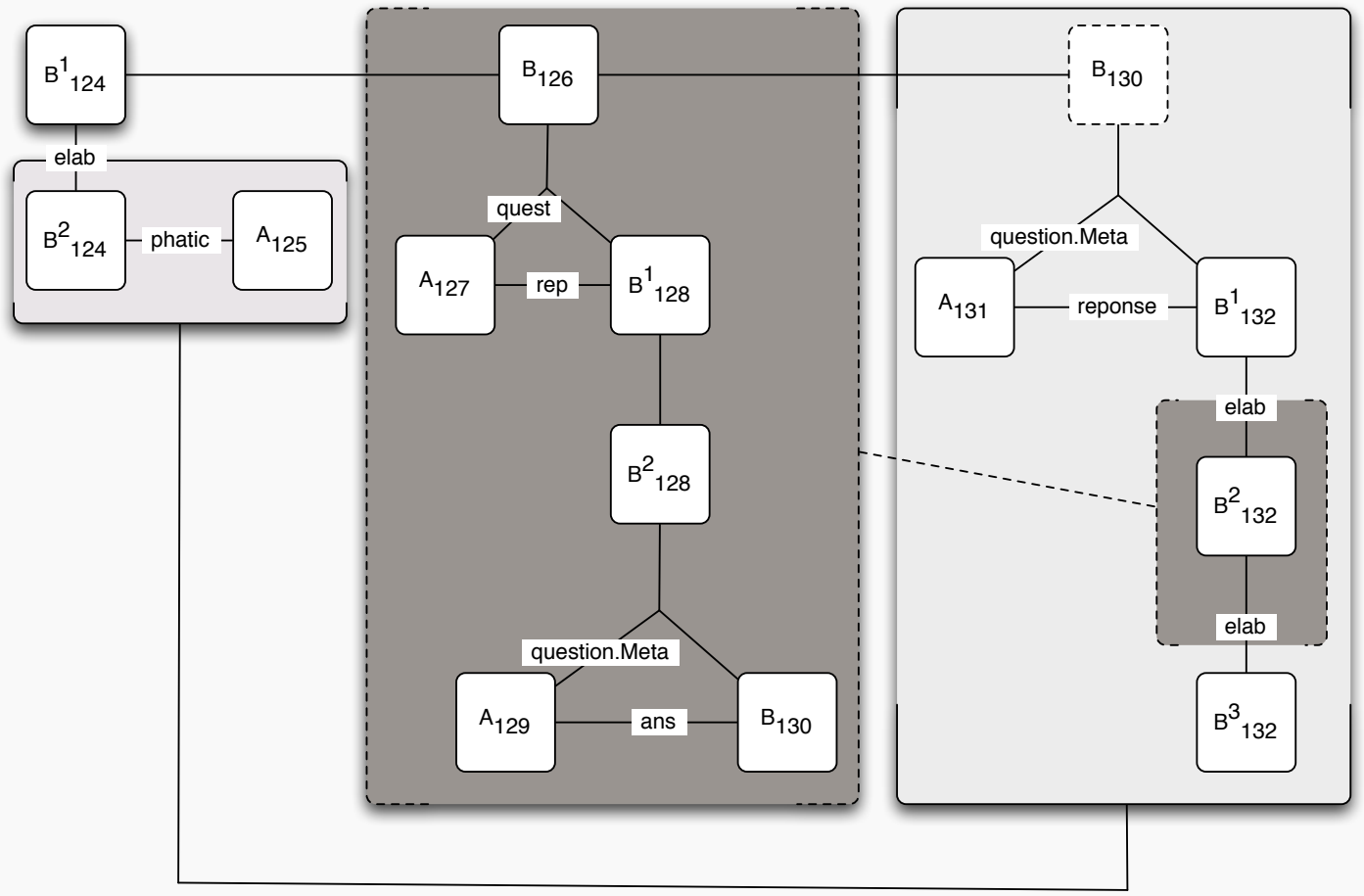
Analyse de la structure logique du dialogue (point de vue patient)

Point de vue du patient



Analyse de la structure logique du dialogue (point de vue psy)

Point de vue du psychologue



Application à l'aide au diagnostic de la schizophrénie

- Etudes de dialogues psychiatre/patient
- Discours logiquement cohérent
- Mais modification/superposition d'interprétations à un endroit de la structure discursive ou dialogique où on ne peut le faire sans le préciser:
  - De référents (par ex. deux personnes portant le même prénom)
  - De deux sens d'un mot (par ex. « mort » sens figuré / sens propre)
- Une analyse automatique peut déceler ce phénomène assez caractéristique de cette pathologie, et cela peut aider au diagnostic.

La logique AUJOURD'HUI au LIRMM

Principalement, mais pas seulement:

Calculabilité

Vérification, preuves de programmes

Représentation des connaissances

Sémantique du langage naturel

Action transverse « logique » depuis un an.