Part 1. Histoire de λ-calcul

Qu'est-ce que c'est un λ-calcul ? Les codeurs sont familiers avec une notion de λ-fonction - une fonction anonyme qui est utilisée dans les morceaux du code qui ne méritent pas d'avoir un méthode nommé : clé de trie, les petits transformation dans les requêtes à la sql etc. Cépendant, la notion de λ-fonction a été pris d'une système de calcul aussi puisant que la machine de Turing (est inventé dans les mêmes années 30s). Dans cet article on va discuter l'histoire de son invention pour mieux comprendre le concept.

Plan

1. Crise des fondaments
2. Axiomes de Peano
3. 1ere version de Lambda calculs
4. Theoreme de Goedel
5. Machine de Turing et calculabilité
6. Thèse de Church-Turing
7. Impact et applications

Crise des fondaments

Qui n'a jamais vu cette phrase : *"Cette phrase est fausse"* ? Probablement, personne. Tout le monde sait qu'elle n'est ni vrai ni fausse (effectivement, s'il on suppose qu'elle est vrai, alors elle doit être fausse et à l'invers). Connue depuis presque 3000 ans sous un nom d'un paradoxe du menteur, les mathématiciens ont eu une habitude de vivre avec jusqu'à la fin de XIXème siècle. Cépéndant, les "invités inattandus" ont arrivés de temps en temps :

- **Paradoxe du barbier.** Un barbier rase tous qui ne se rasent pas eux-mêmes et seulement ceux-ci; Qui rase ce barbier ?
- **Paradoxe sorite.** Un grain isolé ne constitue pas un tas. L'ajout d'un grain ne fait pas d'un non-tas, un tas. Donc on ne peut pas construire un tas par l'ajout des grains.
- **Paradoxe du crocodile.** Un crocodile méchant vous attrape et propose de deviner votre déstin. Si votre devine est incorrecte, il vous mange. La réponse ? – "Tu vas me dévorer" !

Pour une liste exhaustive des paradoxes simples, on peut consulter un livre de Martin Gardner. "Aha! Gotcha. Paradoxes to puzzle and delight". Maintenant, discutons un autre saboteur de logique : *Paradoxe de l'ensemble de Russel*. Disons qu'un ensemble est *simple* s'il n'appartient pas à lui-même. Par exemple, l'ensemble des tout les gens est simple, car cet ensemble n'est pas une personne. Ainsi, l'ensemble des tout les ensemble n'est pas simple par son définition. *L'ensemble de Russel* est un ensemble qui contient tout les ensembles simples et rien d'autre. Est-ce qu'un ensemble de Russel est simple ? Si c'est le cas, par construction il contient lui-même. Donc il n'est pas simple. Mais s'il n'est pas simple il doit contenir lui-même, ce que signifie qu'il est simple. *Contradiction*.

Les mathématiciens n'étude pas ni crocodiles, ni barbiers. Les questions des menteurs sont plutôt les compétences de code penal ou les philosophes. Cépendant dans une version de Russel ce paradoxe n'utilise que les constructions formelles de mathématique. Cela signifie que telles constructions sont contradictoires elles-mêmes : si nous avons prouvé qu'une formule propositionnelle est à la fois vrai et fausse, le même peut avoir lieu pour n'importe quel théorème. Si on ajoute qu'au début de XXème siècle paradoxe de Russel n'a pas été le seul paradoxe connu, on voit bien qu'est-ce que c'était le *crise de fondaments* en mathématique.

Ce crise a été refleté sous le numéro 2 dans une liste des 23 fameux problèmes de Hilbert détérminants le développement du mathématique en XXème siècle.

2ème problème de Hilbert *Déterminer la consistence de l'arithmétique.*

Dans le sens plus formel, la consistence signifie le suivant.

1. Il y a des axiomes dont on peut déduire tout les théorèmes de l'arithmétique.
2. Aucun axiomes ne peut pas être déduit des autres.
3. Il n'existe pas d'une proposition X, tel que les axiome implique X ainsi que "non X".

L'étape 1 est plutôt constructif : en pratique, il est suffisant de produire les nombres (entiers, rationnels, réels) avec ses propertés habituels. Dans l'étape 2 il faut prouver que les axiomes sont indépendants l'un des autres. Équivalentment, si on supprime n'importe quel axiome, l'étape 1 n'est plus vrai. L'étape 3 est le plus compliqué.

Axiomes de Peano

L'arithmétique est un domain de mathématique qui étude les nombres et rélations entre eux. Elle est appliquée partout de premiers années de l'école

jusqu'à les conceptes modernes d'astrophysique. Cépendant, pour construire les bases de l'arithmétique, il est presque suffisant de bien déterminer les nombres naturels ainsi que les action qu'on peut faire avec. (Les nombres entiers est une extension pour que opération $x-y$ renvoit toujours un nombre valide, les nombres rationnels aparaissent si on étudie la division. Finalement, les nombres algébrique sont résponsable pour résoudre les équatinos polynomials et le reste - pour "fermer des trous"). Classiquement, les nombres naturels peuvent être définis de même façon qu'on fait quand les petits enfants apprennent à compter: ce résultat est connus dépuis la find de XIXème siècle comme les axiomes de Peano:

1. 1 est naturel;
2. le nombre suivant d'un nombre naturel est naturel;
3. rien ne suivi de 1;
4. si a suive b et a suive c, alorc $b = c$;
5. axiome de recurrence (i.e., si un prédicat $A(x)$ est vrai pour $x = 1$ ainsi que $A(n)$ implique $A(n + 1)$, alors $A(x)$ est vrai pour tout n naturel).

Montrons que avec ces axiomes sont suffisant pour construire tout les nombres.

- **Nombres naturels** sont déjà construit. Ok, pour être honête, nous avons construit les objets "bizzares" et les avons appelés les nombres naturels – prenez l'habitude que mathématique fondamental est une façon de parler des choses évidents depuil l'école avec des mots très sophistiqués. Mais la vrai avantage de cet approche est son **correctité** absolu.

- **Zero** est indispensable pour compter. Rien plus simple - ajoutons un objet nouveau spéciale, qui est (i) suivi de 1. Appelons lui "0". Posons que pour tout n naturel (ii) $n+0 = 0+n = n$ et aussi (iii) $n\cdot 0 = 0\cdot n = 0$ (servira pour le futur).

- On peut compter et même calculer la somme, mais les mathématiciens veulent plus de symmetrie, donc l'opération réciproque de "+" doit exister. D'accord: par définition, la différence $a-b$ est un nombre c tel que $a = b+c$. Que vaut 2 - 5? Oups, il n'existe pas tel c que $c + 5 = 2$ - n'oubliez pas qu'on veut la strictité absolue, donc on ne peut utiliser que des nombres déjà calculés. Nous n'avons pas de choix: disons que "2 - 5" et un nouveau nombre. Ainsi que "1 - 2", "42 - 45" et même

"239 - 261". Cela semble beaucoup, mais remarquons que 2 - 5 est égal au 42 - 45 et aussi au 0 - 3. Pour simplicité, omittons zero et écrivons juste -3. Félicitations ! Vous venez de construire les nombres **négatifs** et donc les nombres **entières** ! Cet opération s'appelle la **closure** et est très typique pour la génération des nouveaux objets.

- Les **nombres rationnels** arrivent par la même logique que : si nous pouvons calculer le produit, alors nous voulons diviser. Les résultats de tout les divisions possibles (1/2, -2/3, 2/4, 37/17, 5/5, etc.) forment les nombres rationnels – vous devez le souvenir bien depuis l'école - d'habitude ils sont appris plus tard que les nombres négatifs.

- Imaginons l'axe de nombres. D'un point de vue, il est très dense – pour n'importe quel nombre rationnel, il existe un autre nombre rationnel qui est "autant proche de lui qu'on veut". Il n'est pas suffisant ! Malheureusement, $\sqrt{2}$ n'est pas rationnel (à propos : 7ème problème de Hilbert s'agit de prouver que $\sqrt{2}^{\sqrt{2}}$ n'est pas rationnel). Donc les **nombres réels** sont définit par une autre closure. Informellement on rempli des "trous" sur l'axe des nombres. Pour les plus curieux qui souhaitent la construiction formelle, la page de wikipedia est bien explicatif. Personnellement, je prefère la construiction par des coupes de Dedekind.

todo: introduce the main manipulations for the lambda, combinators, SKI

Heureusement, la vraie preuve d'une consistence des axiomes de Peano est un problème beaucoup plus sophistiqué que l'invention de ses axiomes, et l'histoire n'est donc que commencée.

1ère version de Lambda calcul

En 1932 Church a proposé une autre construction qui est connue comme **λ-calcul non-typé**. Malheureusement, son étudiant, Kleene a prouvé que cette construction n'a pas été consistente.

λ-calcul a formalisé une application d'une fonction. L'écriture envisage la compréhension d'une fonction comme une "règle". Et l'écriture classique $f(x)$ pointe plutôt sur le résultat de ce règle.

Rappelon brièvement, qu'est ce que c'est. (Sinon, wiki et les autres articles ou "Eggs and crocodiles") Le brique principal est une fonction. Au lieu de $f(x)$ on écrit $\lambda x.f$. Si on parle de la valeur de $f(x)$ quand $x = a$, on écrit $\lambda x.fa$. Naturelement, ion peut définir une composition... Pour transformer des propositions on a une règle de β-reduction.

Malgré sa simplicité et abstraité, cette construction permet néanmoins rédefinir tout les opérations arithmétiques, la logique Booléen etc. Est-ce que λ-calcul non-typé est un bon candidat pour le rôle de fondament de mathématique ? La réponse est **non**: à cause de Paradoxe de Kleene-Rosser proposé en 1935 par J. B. Rosser et Stephen Kleene qui a été un étudiant de Church.

Ironiquement, ce paradoxe, beaucoup plus sophistiqué dans sa version initiale, n'a pas très loin des paradoxes plus simples décrites au début de cet article. Commençons par une phrase "si cette phrase est vraie, alors X", où X est un énoncé quelconq.

- Par le propriétés d'implications ("faux =¿ X" est toujours vrai), cette phrase ne peux pas être faux.
- S'il est vrai, alors X est vrai.
- Nous venons de prouvé que n'importe quel enoncé est vrai, e.g. les États-Unis et la Chine ont une frontière commune (ce que peut probablement expliquer la construction de "The Great Wall").

Il peut être formulé en termes de λ-calculs. Mais la "rootcause" de tout les paradoxe de ce type est la même – l'autoréférence : la phrase entière est contenu dans sa première motié. Remarquons qu'intérdire les autoréférences dans la logique n'est pas la solution parfaite, car la logique devient trop restrente par rapport au langage naturelle.

Considerons une fonction r définie comme $r = \lambda x.((xx) \to y)$. (rr) β-se réduit en $(rr) \to y$. Si (rr) est faux, alors $(rr) \to y$ est vrai par le principe d'explosion, mais cela est contradictoire avec la β-réduction. Donc (rr) est vrai. On en déduit que y est aussi vrai. Comme y peut être arbitraire, on a prouvé que n'importe quel proposition est vrai. Contradiction.

Théorème de Gödel

Les deux paradoxes discutés ci-dessus, sont basés sur le même concept de l'autoréférence : une proposition ou n'importe quel objet qui réference lui-même (e.g., ensemble des tout les ensembles). Faut-il intérdir l'autoréference dans les constructions mathématiques ? L'idée n'est pas séduisant si on rappel que avec les paradoxes, nous avons jeté dans la poubelle tout les construcitons récursives.

Néanmoins, l'autoréférence a une influence forte sur le fondement de mathématique. Un résultat clé et le plus connu comme la théorème de l'incomplétude a été prouvé par Kurt Gödel en 1930. Une des intérpretations

prétends que la consistence d'une système d'axiomes ne peut pas être prouvée en n'utilisent que ces axiomes (voici l'autoréference !). En particulier, pour prouver la consistence d'arithmétique il faut ajouter les axiomes supplémentaires (qui a été vite fait, en 1936). Le seul problème est que maintenant il faut prouver une autre système...

Pour ceux qui veulent plonger dans le sujet de l'autoréférence, nous pouvons conseiller un livre "Gödel, Escher, Bach : Les Brins d'une Guirlande Éternelle" de Douglas Hofstadter.

La crise des fondements a déclenché plusieurs études sur le sujet. Nous avons brièvement présenté deux modèles qui ont été les candidats sur le rôle de base minimale de l'arithmétique. Cépéndant, le λ-calcul non typé est contradictoire car il contient des paradoxes. La consistence de l'arithmétique Péano a été prouvé un an après, en utilisant la récurrence transfinie par Gerhard Gentzen. D'après le théorème de Gödel, l'ajout d'un proposition supplémentaire dans le système des axiomes a été nécessaire. C'était une idée qui a été manquant pendant presque 50 ans entre la publication des axiomes de Péano et la preuve de Gentzen.

Pour résumer le sujet de l'arithmétique, disons que dans la version moderne on construit le fondement toujours à partir des axiomes de Péano. Pour la consistence, au lieu de la récurrence transfinie, on rajout la théorie des ensemble de Zermelo-Fraenkel avec l'axiome de choix. Néanmoins, chez les mathématiciens il n y a pas de consensus si le deuxième problème de Hilbert est résolu ou non.

Machine de Turing et calculabilité

Cépéndant, comme il est souvent en science, il faudrait étudier le même domaine de point de vue un peu différent. Cela a été fait sur l'autre continent par un jeun étudiant Alan Turing. Il a cherché une solution pour une problème de la décision posé en 1928 par Hilbert et Ackermann : "trouver un algorithme qui détermine dans un temps fini, s'il un énoncé est vrai ou faux". La formalisation d'un terme algorithme a conduit au concept de machine de Turing connu par tout le monde. Entre outre, le théorème de Gödel a été reformuler en thermes d'une machine de Turing. Le résultat a été aussi négative, connu comme une théorème de Turing-Church: "il existe les énoncés pour lesquels on ne peux pas déterminer" (vérifier l'enoncé et le nom d'un théorème).

Thèse de Church-Turing

Le résultat positif. S'il existe les fonctions, qu'il peuvent pas être décidées, on se pose la question, qu'est-ce que ce sont les fonction simple, i.e. les fonctions que l'on peut effectivement calculer. Intuitivement, c'est dont la valeur peut être calculée avec un crayon si on a suffisament de papier et du temps. Mais vous comprenez déjà que les mathématiciens n'acceptent pas les solutions intuitives... Le problème de décision est lié avec une problème de calculabilité. Qu'est-ce que signifie qu'une fonction peut être calculée ? Souvent on se refère sur "des méthodes d'un crayon et de papier". Indépendement, chaque des deux a proposé que toute fonction calculable en thèrmes de crayon et papier peut être calculé par son méthode (lambda-calcul ou la machine de Turing). Les deux propositions - ne sont pas les théorèmes, peuvent pas être prouvées car on ne peut pas formaliser autrement calculabilité. (On doit remarquer ici qu'il y avait le troisième mechanisme de détérminer la calculabilité - les fonction récursive primitive). Relativement vite il a été prouvé que tout les 3 méchanismes sont équivalent. Donc, n'importe lequel peut être utilisé comme une définition de function effectivement calculable.

Résumé. Impacts de λ-calcul

Le concept de λ-calcul a joué une rôle tellement importante dans l'informatique théorique que l'on peut voir ses échos en pratique : dans la plupart des langages de programmation une notion de λ-fonction représente une fonction "anonyme". Cette notion rends la terme connue par des ingénieurs mais la plupart ne connaît pas les détails cachés derrière. Cela provoque souvent les discussions dans StackOverflow similaire à celui-ci: *"Another obvious case for combinators is obfuscation. A code translated into the SKI calculus is practically unreadable. If you really have to obfuscate an implementation of an algorithm, consider using combinators, here is an example."*

En réalité le concept a eu quatre impacts principaux.

1. *Formalisation d'une notion de calculabilité.* Avant les années 1930s, la définition de calculabilité pouvait être caricaturisée comme "calculable à l'aide du papier, crayon et suffisament du temps". En plus il y avait une intuition que les fonctions récursives doivent définir la classe des fonctions calculables. L'invention de λ-calcul et machine de Turing a relancé une discussion sur la notion de calculabilité. Comme tout les trois concept ont été prouvés équivalents, les mathématiciens se sont mis d'accord a les utiliser comme une définition formelle de calculabilité.

2. *Preuves de calculabilité.* Car les trois concept sont équivalents, n'importe lequel peut être utilisé pour prouver la calculabilité d'un nouvaux objet. Donc on peut considerer λ-calcul comme un outil de plus (en réalité outilisé plus souvant pour prouver qu'un objet est n'est pas calculable).

3. *Preuves formelles.* La version des λ-calcul typés peut être appliquée dans la théorie des preuves. Ainsi, les certains langages de preuves formelles tels que Coq ou AUTOMATH sont basés sur ce modèle.

4. λ-calul est un *langage de programmation* primitif (en nombre de constructions). Comme la machine de Turing est le fondament de tout les langages impératifs, λ-calcul est une base pour les langages fonctionnels tels que Haskell ou OCaml.

Part 2. Les formalités.

What is λ?

[1] En mathématique la notion d'une fonction est liée avec une application, i.e., règle qui transform paramètre dans un résultat. Au contraire, λ-calcul est une théorie des "fonctions comme formules". La différence est ce que une formule formelle n'est pas obligatoirement se traduit en règle bien précise. Commençons par un exemple. En arithmétique on peut écrire :

$$\text{Soit } f \text{ est une fonction } x \to x^2. \text{ Considerons } A = f(5).$$

En langage de lambda, on peut écrire simplement:

$$(\lambda x.x^2)(5).$$

L'expression $\lambda x.x^2$ signifie une fonction qui mappe x à x^2. Puis ce terme est succédé par une *application* de cette fonction au nombre 5. L'un des avantage de cette notation est simplicité dans la construction des fonctions de l'ordre supérieur : si $f : X \to X$ est une fonction, alors la composition $f \circ f$ peut s'écrire comme $\lambda x.f(f(x))$. Ceci n'est pas simple, mais l'opération qui mappe f à $f \circ f$ s'écrit méchaniquement de manière suivante :

$$\lambda f.\lambda x.f(f(x)).$$

(On peut le comparer avec $g : (X \to X) \to (X \to X)$ où $g(f) = f \circ f$ pour tout $f : X \to X$.) Le vrai avantage est visible si on considère un terme f

[1] based on Selinger's lecture notes

suivant: $\lambda x.x$. Rien inattendu, c'est une fonction d'identité. Mais que vaut $f(f)$? Par définition, si on pose $x = f$,

$$f(f) = (\lambda x.x)(f) = f.$$

Remarquons que $f(f)$ n'a jamais du sens dans mathématique classique car la fonction ne peut pas être inclue dans sa propre domaine de définition.

todo: λ sans type est simplement typé

Combinateurs

Le cas spécial de λ-termes sans type sont les termes qui n'ont pas des variables libres. Ils s'appellent *combinateurs*. Voici les examples des combinateurs classiques :

- $I = \lambda x.x$
- $\omega = \lambda x.xx$
- $\Omega = \omega\omega = (\lambda x.xx)\lambda x.xx$
- $K = \lambda xy.x$
- $K_* = \lambda xy.y$
- $C = \lambda fxy.fyx$
- $B = \lambda fgx.f(gx)$
- $S = \lambda fgx.fx(gx)$

Chaque combinateur peut être appliqué aux autre tèrmes, par exemple :

- $I\mathcal{x} = \mathcal{x}$
- $\omega\mathcal{x} = \mathcal{x}\mathcal{x}$
- $K\mathcal{x}\mathcal{y} = \mathcal{x}$
- $Sfg\mathcal{x} = f\mathcal{x}(g\mathcal{x})$

Les formules ci-dessus peuvent s'en servir tant que la définition des combinateurs. Le calcul est effectué en remplaçant les arguments formels par ses valeurs, e.g.,

$$\omega I = II = I$$

. Notons, que les certains combinateurs peuvent être exprimé en termes des autres. (**todo**) Si on choisit une base, e.g., S, K (et I tant que un élement neutre), on peut obtenir un système de calcul qui est équivalent au λ-calcul.

Prise en main[2]

Dans *lambda*-calcul sans type nous n'avons qu'un seul primitif - des fonctions. Dons, si on veut l'utiliser pour la programmation, c'est à nous de réaliser même les objets les plus élementaires, tels que les nombres ou les constantes booléennes.

$tru \quad := \lambda t.\lambda f.t \quad$ est une fonction qui renvoie son premier argument,
$fls \quad := \lambda t.\lambda f.t \quad$ est une fonction qui renvoie son deuxième argument.

Les termes tru et fls vont jouer le rôle de **vrai** et **faux**. Cependant, pour l'instant ils ne sont que des formules formelles qui manquent du context. Comme ce contexte, définissons la fonction if

$$if := \lambda b.\lambda x.\lambda y.bxy$$

Ici, b est une condition de branchement, x et branche **then** et y corresponds à **else**. Donc, pour "montrer" que tru et fls corréspondent au constantes logiques, nous avons besoin de prouver le suivant:

$$\begin{aligned} if\ tru\ t\ e &= t, \\ if\ fls\ t\ e &= e \end{aligned}$$

Pour les formules formelles "prouver" signifie "partir d'une expression à gauche, appliquer les certains règles afin d'obtenir une expression à droit". Donc c'est le moment de parles de ces règles. Pour λ-calcul il y en a deux :

1. α**-equivalence**. Informellement[3], on dit que deux termes sont équivalent s'il coïncident à renommage des variables abstraites près. Par exemple, $\lambda x.f(x) \equiv_\alpha \lambda y.f(y)$. Par une variable abstraite on comprend une variable qui est présente à gauche et à droit du point, e.g., x et y eux-mêmes ne sont pas λ-equivalents car il ne sont pas abstraites.

2. β**-reduction**.

Notons que dans λ-calcul, il n'y a rien sauf application, abstraction et β-equivalence.

[2]Basé sur l'article russe `https://habr.com/ru/post/215991/`

[3]la définition formelle peut être trouvée dans n'importe quel livre, mais sa complexité dépasse largement les objectifs du blog.

Preuve $(if\ fls\ t\ e = e)$.

$$
\begin{aligned}
&(\lambda b.\ \lambda x.\ \lambda y.\ b\ x\ y)\ fls\ t\ e \\
&(\lambda x.\ \lambda y.\ fls\ x\ y)\ t\ e \\
&(\lambda y.\ fls\ t\ y)\ e \\
&fls\ t\ e \\
&(\lambda t.\ \lambda f.\ f)\ t\ e \\
&(\lambda f.\ f)\ e \\
&e
\end{aligned}
$$

□

todo: "and", "or"

Pourquoi langage de programmation?

Recursion à l'aide de combinators